ID: 412657
Sample Name: #Ud83d#Udce0Lori's Fax VM-002.html
Cookbook: default.jbs
Time: 20:49:08
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report #Ud83d#Udce0Lori's Fax VM-002.html 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Sigma Overview 4
Signature Overview 5
AV Detection: 5
Phishing: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 9
Private 9
General Information 9
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 13
JA3 Fingerprints 14
Dropped Files 15
Created / dropped Files 15
Static File Info 43
General 43
File Icon 43
Network Behavior 44
Network Port Distribution 44
TCP Packets 44
UDP Packets 45
DNS Queries 47
DNS Answers 47
HTTPS Packets 48
Code Manipulations 49
Statistics 49
Behavior 49

System Behavior 49
Analysis Process: chrome.exe PID: 1700 Parent PID: 3900 49
General 49
File Activities 50
Registry Activities 50
Analysis Process: chrome.exe PID: 6332 Parent PID: 1700 50
General 50
File Activities 50
Registry Activities 50
Disassembly 51

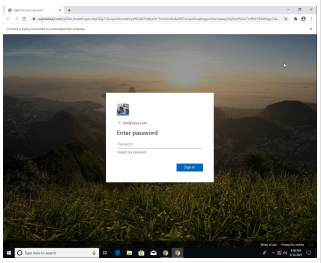
Analysis Report #Ud83d#Udce0Lori's Fax VM-002.html

Overview

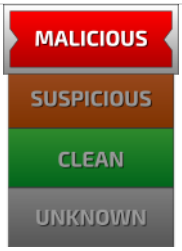
General Information

Sample Name:	#Ud83d#Udce0Lori's Fax VM-002.html
Analysis ID:	412657
MD5:	dd018534b72286..
SHA1:	e304a5ef3e4786c.
SHA256:	3c2937c71e855d..
Infos:	

Most interesting Screenshot:



Detection



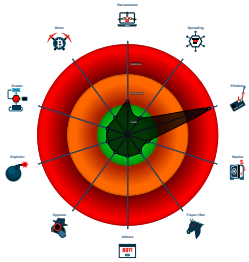
HTMLPhisher

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Yara detected HtmlPhish3
- Yara detected Phisher
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 1700 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\#Ud83d#Udce0Lori's Fax VM-002.html' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6332 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1508,17710434684604522 59,206189002582279930,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1940 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
#Ud83d#Udce0Lori's Fax VM-002.html	JoeSecurity_Phisher_2	Yara detected Phisher	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

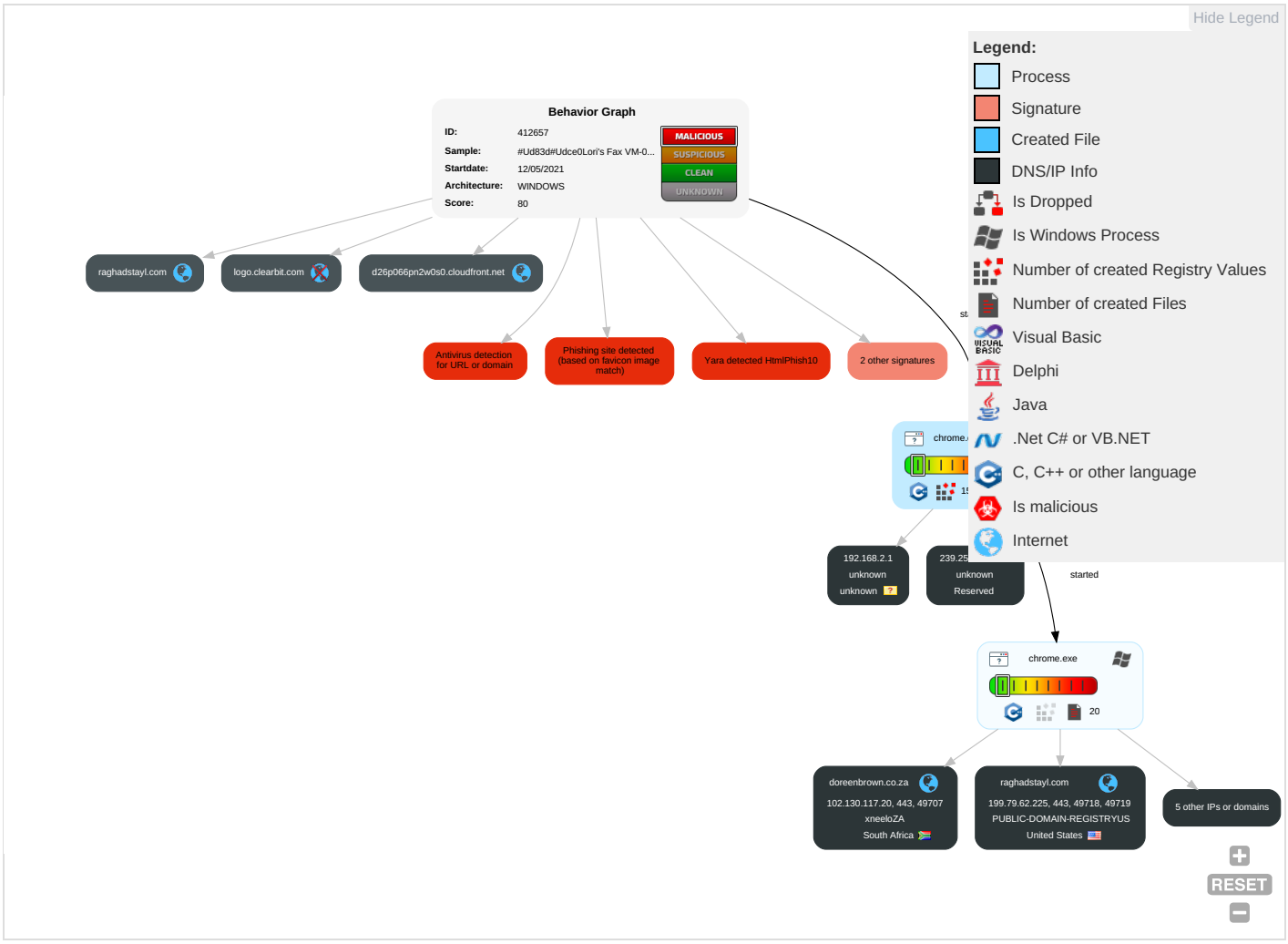
Yara detected HtmlPhish3

Yara detected Phisher

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitior
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

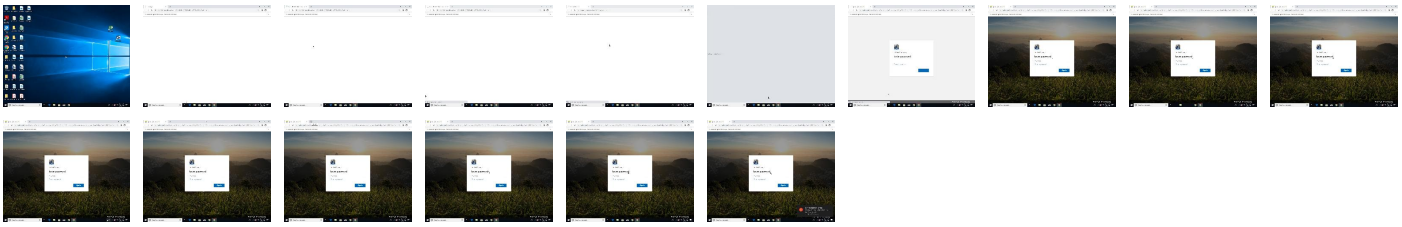
Behavior Graph

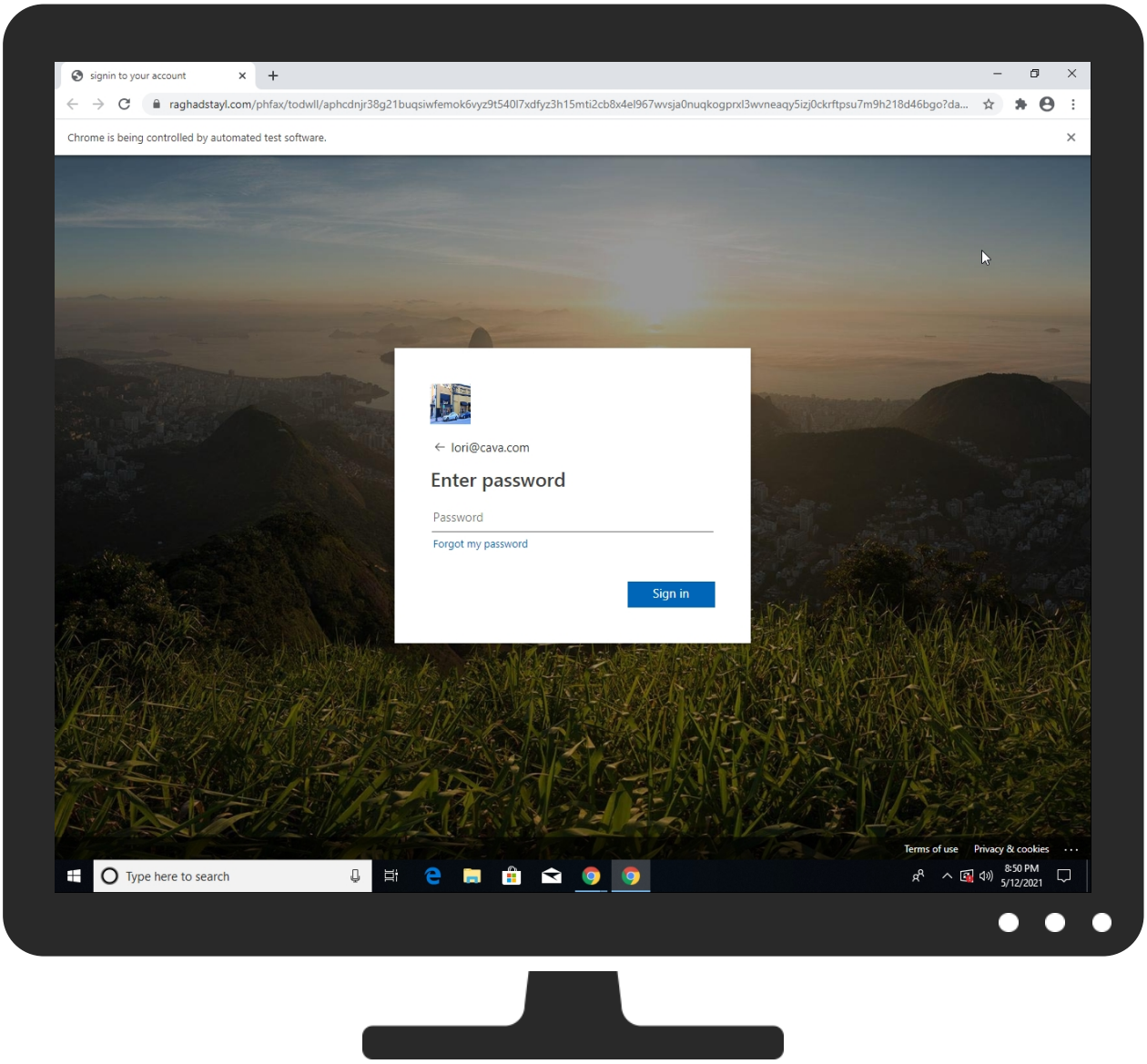


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://raghadstayl.com/phfax/todwll/aphcdnjr38g21buqsiwfemok6vyz9t540l7xdfyz3h15mti2cb8x4el967wvsja0nuqkogprxl3wvneaqy5izj0ckrftpsu7m9h218d46bgo?data=bG9yaUBjYXZhLmNvbQ==	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://raghadstayl.com/phfax/todwll/bG9yaUBjYXZhLmNvbQ==signin	0%	Avira URL Cloud	safe	
http://https://raghadstayl.com/phfax/todwll/bG9yaUBjYXZhLmNvbQ==	0%	Avira URL Cloud	safe	
http://https://raghadstayl.com/phfax/todwll/images/favicon.ico	0%	Avira URL Cloud	safe	
http://https://raghadstayl.com/phfax/todwll/aphcdnjr38g21buqsiwfemok6vyz9t540l7xdfyz3h15mti2cb8x4el967wvsja	0%	Avira URL Cloud	safe	
http://https://raghadstayl.com	0%	Avira URL Cloud	safe	
http://https://raghadstayl.com/phfax/todwll/bG9yaUBjYXZhLmNvbQ==2	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d26p066pn2w0s0.cloudfront.net	13.224.193.12	true	false		high
doreenbrown.co.za	102.130.117.20	true	false		high
raghadstayl.com	199.79.62.225	true	false		unknown
googlehosted.l.googleusercontent.com	216.58.212.129	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
logo.clearbit.com	unknown	unknown	false		high

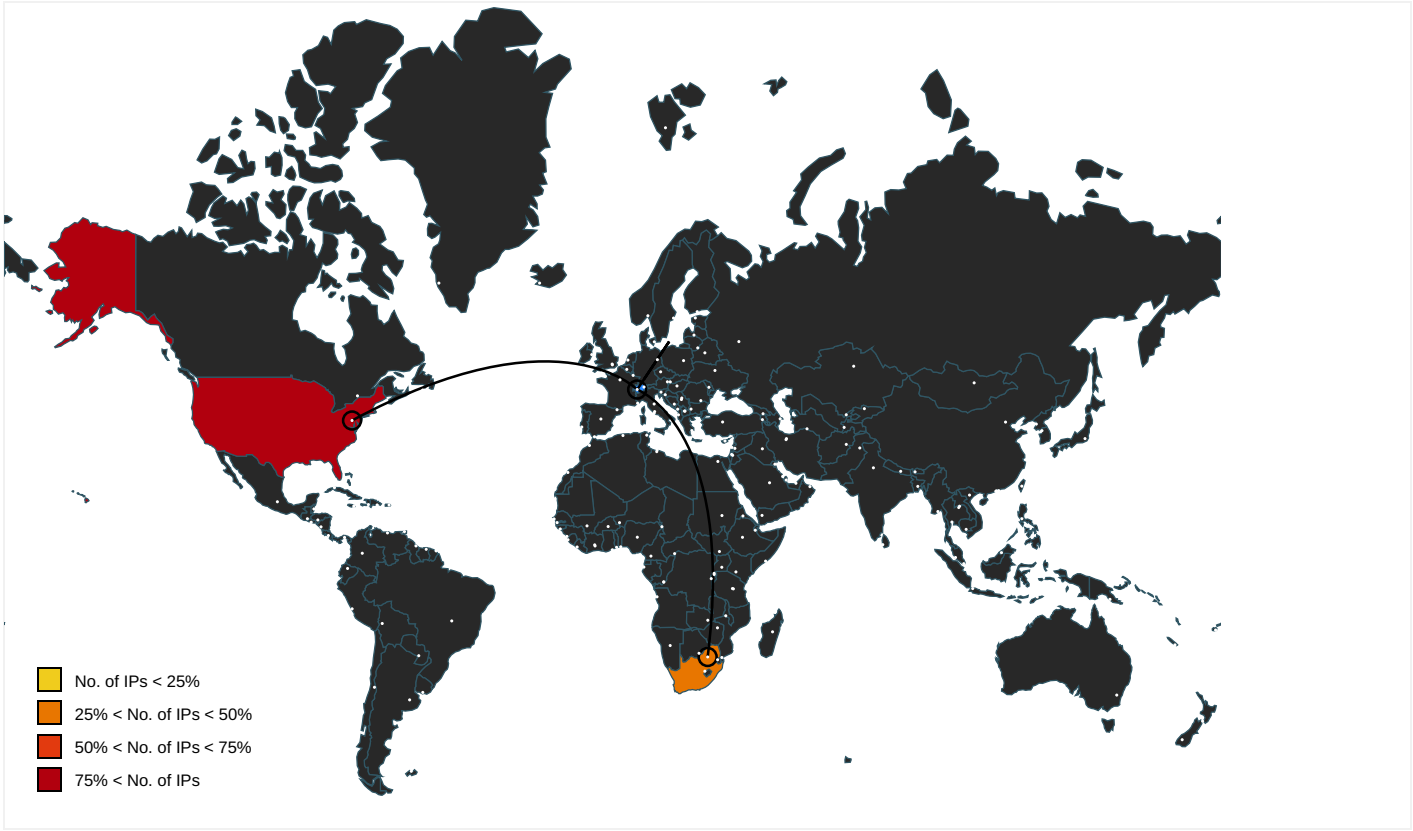
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://raghadstayl.com/phfax/todwll/aphcdnjr38g21buqsiwfemok6vyz9t540l7xdfyz3h15mti2cb8x4el967wvsja0nuqkogprxl3wvneaqy5izj0ckrftpsu7m9h218d46bgo?data=bG9yaUBjYXZhLmNvbQ==	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	4fd2613b-1edf-4333-9a79-0ba77e88f48e.tmp.3.dr, 5ea0e6f8-9224-475c-9543-23cce0815b5d.tmp.3.dr, 2c9daf34-360e-47e3-bd47-7cb8fb610dda.tmp.3.dr, 4d68cbbb-c5c6-4205-b99f-92b08a650e3e.tmp.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://raghadstayl.com/phfax/todwll/bG9yaUBjYXZhLmNvbQ==signin	History.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://raghadstayl.com/phfax/todwll/bG9yaUBjYXZhLmNvbQ==	Favicons.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://raghadstayl.com/phfax/todwll/images/favicon.ico	Favicons.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://logo.clearbit.com	4fd2613b-1edf-4333-9a79-0ba77e88f48e.tmp.3.dr	false		high
http://https://raghadstayl.com/phfax/todwll/aphcdnjr38g21buqsiwfemok6vyz9t540l7xdfyz3h15mti2cb8x4el967wvsja	History.1.dr, History Provider Cache.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://raghadstayl.com	4fd2613b-1edf-4333-9a79-0ba77e88f48e.tmp.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://doreenbrown.co.za/tele/cd/?lori	History.1.dr, History Provider Cache.1.dr	false		high
http://https://clients2.googleusercontent.com	4fd2613b-1edf-4333-9a79-0ba77e88f48e.tmp.3.dr, 5ea0e6f8-9224-475c-9543-23cce0815b5d.tmp.3.dr	false		high
http://https://raghadstayl.com/phfax/todwll/bG9yaUBjYXZhLmNvbQ==2	History Provider Cache.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://doreenbrown.co.za	Current Session.1.dr	false		high
http://https://feedback.googleusercontent.com	manifest.json0.1.dr	false		high
http://https://doreenbrown.co.za/tele/cd?lori	History.1.dr, History Provider Cache.1.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.79.62.225	raghadstayl.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
216.58.212.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
102.130.117.20	doreenbrown.co.za	South Africa		37153	xneeloZA	false
13.224.193.12	d26p066pn2w0s0.cloudfront.net	United States		16509	AMAZON-02US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412657
Start date:	12.05.2021
Start time:	20:49:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	#Ud83d#Udce0Lori's Fax VM-002.html
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.phis.winHTML@40/230@6/7
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .html

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 20.82.209.183, 93.184.220.29, 52.147.198.201, 13.64.90.137, 142.250.184.195, 142.250.185.110, 216.58.212.173, 142.250.185.206, 95.168.222.144, 95.168.222.76, 67.26.137.254, 8.241.126.121, 8.253.207.121, 8.241.79.254, 8.238.85.254, 23.57.80.111, 34.104.35.123, 142.250.186.42, 142.250.186.74, 142.250.186.106, 142.250.186.138, 142.250.186.170, 142.250.184.202, 142.250.184.234, 172.217.18.106, 172.217.23.106, 216.58.212.138, 142.250.185.74, 172.217.16.138, 142.250.185.106, 142.250.185.138, 142.250.185.170, 142.250.185.202, 92.122.145.220, 2.20.143.16, 2.20.142.209, 216.58.212.131, 172.217.16.131, 92.122.213.194, 92.122.213.247, 20.82.210.154, 95.168.222.16, 20.50.102.62, 20.54.26.129, 52.155.217.156 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, clientservices.googleapis.com, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, clients2.google.com, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, update.googleapis.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, r5.sn-n02xgoxufvg3-2gbs.gvt1.com, ris-prod.trafficmanager.net, r1.sn-n02xgoxufvg3-2gbl.gvt1.com, www.googleapis.com, r5---sn-n02xgoxufvg3-2gbz.gvt1.com, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, edgedl.me.gvt1.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, clients.l.google.com, au.download.windowsupdate.com.edgesuite.net, r1---sn-n02xgoxufvg3-2gbl.gvt1.com, store-images.s-microsoft.com-c.edgekey.net, r5---sn-n02xgoxufvg3-2gbs.gvt1.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, r5.sn-n02xgoxufvg3-2gbz.gvt1.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, redirector.gvt1.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, skypedataprdcolwus17.cloudapp.net, accounts.google.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, skypedataprdcoleus16.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/412657/sample/#Ud83d#Udce0Lori's Fax VM-002.html

Simulations

Behavior and APIs

Time	Type	Description
20:50:11	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
13.224.193.12	#U260e#Ufe0fAUDIO-2020-05-26-18-51-m4a_MP4messages_2202-434.htm	Get hash	malicious	Browse	
	Ctr-8602985_xls.Html	Get hash	malicious	Browse	
	http://https://firebasestorage.googleapis.com/v0/b/mdhghfbfggdndgfdvnd.appspot.com/o/index1.html?alt=media&token=d97d4868-2770-48a4-b497-20b5cf4d5cc9&email=judy.fabre@nrgenergy.com&domain=judy.fabre@nrgenergy.com	Get hash	malicious	Browse	
239.255.255.250	INV-Receipt.html	Get hash	malicious	Browse	
	ATT82166.HTM	Get hash	malicious	Browse	
	#Ud83d#Udd7b Missed Playback Recording.wav - 1424592794.htm	Get hash	malicious	Browse	
	rG7hoAI6Ke.exe	Get hash	malicious	Browse	
	Remittance Copy 550469 - jessica.taylor@granburyisd.org.html	Get hash	malicious	Browse	
	Wave Browser_ajpko2tb_.exe	Get hash	malicious	Browse	
	schreiberfoods paymentMay 10, 2021, 0616 AM EDT.hTMl	Get hash	malicious	Browse	
	Open_Invoice_and_statements.htm	Get hash	malicious	Browse	
	svchost.exe	Get hash	malicious	Browse	
	Wave Browser_cg5vc6cx_.exe	Get hash	malicious	Browse	
	V___oic_____ePl_a_ybac___k for___ ___Bsakhitab_____Varde.htm	Get hash	malicious	Browse	
	Wave Browser_cg5vc6cx_.exe	Get hash	malicious	Browse	
	VM_u7u8-2.html	Get hash	malicious	Browse	
	#U6807#U724c#U6e2f#U7ec8#U7aef.exe	Get hash	malicious	Browse	
	-Remmittance-.htm	Get hash	malicious	Browse	
	A&A Safety, Inc.HTML	Get hash	malicious	Browse	
	ACH Payment.html	Get hash	malicious	Browse	
	#U260e#Ufe0f PAudioMessage_8211-911.htm	Get hash	malicious	Browse	
	Pending DHL Shipment Notification.html	Get hash	malicious	Browse	
	test.html	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
d26p066pn2w0s0.cloudfront.net	Report000042.htm	Get hash	malicious	Browse	• 13.224.193.89
	#U260e#Ufe0f PAudioMessage_8211-911.htm	Get hash	malicious	Browse	• 13.32.21.111
	ACH Payment copy.html	Get hash	malicious	Browse	• 13.224.193.103
	hartmann.info-Pending-messages-07.html	Get hash	malicious	Browse	• 65.9.73.111
	Voicemail sound attachment.HTM	Get hash	malicious	Browse	• 143.204.209.96
	Cloudbest-REQUEST.htm	Get hash	malicious	Browse	• 143.204.209.96
	398473874.html	Get hash	malicious	Browse	• 13.32.25.101
	Payment Report.html	Get hash	malicious	Browse	• 13.32.25.43
	SOC_0#7198, INV#512 Via GoogleDocs gracechung.html	Get hash	malicious	Browse	• 143.204.11.45
	BR-415364.htm	Get hash	malicious	Browse	• 52.84.148.48
	BR-278630.htm	Get hash	malicious	Browse	• 52.84.148.85
	Pds-ch-UPDATE.htm	Get hash	malicious	Browse	• 143.204.11.4
	RemittanceAdvice-000010434.htm	Get hash	malicious	Browse	• 143.204.2.94
	TICKET#030599_Stanfordhealthcareserv.htm	Get hash	malicious	Browse	• 143.204.2.94

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	658908343Bel.html	Get hash	malicious	Browse	• 143.204.2.88
	658908343Bel.html	Get hash	malicious	Browse	• 143.204.2.94
	PolicyUpdate.htm	Get hash	malicious	Browse	• 143.204.202.86
	http://recp.mkt91.net/ctt?m=804040&r=Njg0NjYxMDU1NQS2&b=0&j=NjAwMDczOTg3S0&k=NCLogo&kx=1&kt=12&kd=http://silverphoto.my1.ru/go?https://u2ll1.csb.app#david.alvey@jomaxgb.us	Get hash	malicious	Browse	• 13.224.196.53
	http://www.663915-7531.wdfilmworks.com/1/exrobotosv4/am9uLm1hcnNoYWxsQGJyaXRpc2hnYXMuY28udWs=	Get hash	malicious	Browse	• 65.9.68.128
	http://https://u19684446.ct.sendgrid.net/ls/click?upn=ExCkaDW5fRF4b0-2BdFzzXOpGVxUmUBkTQVDYtz6-2F-2F6sQpB9ec4YeTvc-2FPnUnDIMDIb2AubMzHga4hpNymDGbgcQ-3D-3DzXHV_gseYrccm3Yg9g0U-2Fb6V-2FwOEfVhEyzfJUY9CKuT6j1x6hD-2BVD-2FXrrL753UneC8JwdlSdsJxeT4uZO2-2FnkyzzY-2FV4KbpQiqBePez19ri47JFNd1qeGYdXzsneczJdxIKZq6YKBiHln2o-2BHlyeGrx7mmd-2FKEF6vDKuYmaVkkahRHIdR6pgQGZ4Xb00Ac-2FmtYPK8xGHgIeKMLtkPB0f7wUUc0nz2xc91qH5nUCgfdkLP-2ByM-3D	Get hash	malicious	Browse	• 13.224.93.64

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	1cec9342_by_Libranalysis.exe	Get hash	malicious	Browse	• 44.227.76.166
	595e3339_by_Libranalysis.dll	Get hash	malicious	Browse	• 13.225.75.73
	GmCEpa2M7R.dll	Get hash	malicious	Browse	• 13.225.75.73
	New-Order 04758485.exe	Get hash	malicious	Browse	• 3.16.197.4
	350969bc_by_Libranalysis.exe	Get hash	malicious	Browse	• 52.58.78.16
	7bYDInO.rtf	Get hash	malicious	Browse	• 52.210.171.182
	nT5pUwoJSS.dll	Get hash	malicious	Browse	• 54.247.61.18
	1c60a1e9_by_Libranalysis.rtf	Get hash	malicious	Browse	• 44.230.85.241
	Order 122001-220 guanzo.exe	Get hash	malicious	Browse	• 18.219.49.238
	main_setup_x86x64.exe	Get hash	malicious	Browse	• 104.192.141.1
	A6FAm1ae1j.exe	Get hash	malicious	Browse	• 3.138.180.119
	New_Order.exe	Get hash	malicious	Browse	• 75.2.115.196
	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 13.58.50.133
	YDHhjjAEFbel88t.exe	Get hash	malicious	Browse	• 99.83.175.80
	yU7RItYEQ9kCkZE.exe	Get hash	malicious	Browse	• 99.83.175.80
	Shipment Document BL,INV and packing List.exe	Get hash	malicious	Browse	• 52.58.78.16
	4xPBZai06p.dll	Get hash	malicious	Browse	• 13.225.75.73
	0OyVQNXrTo.exe	Get hash	malicious	Browse	• 3.142.167.54
	rAd00Nae9w.dll	Get hash	malicious	Browse	• 13.225.75.73
	DOC24457188209927.exe	Get hash	malicious	Browse	• 13.224.193.2
PUBLIC-DOMAIN-REGISTRYUS	PRODUCT INQUIRY FROM PAKISTAN.exe	Get hash	malicious	Browse	• 208.91.199.224
	tLes2JdtRw.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Malware.AI.4228845530.13946.exe	Get hash	malicious	Browse	• 208.91.199.224
	Letter of Demand.doc	Get hash	malicious	Browse	• 103.21.59.173
	7b4NmGxyY2.exe	Get hash	malicious	Browse	• 162.215.241.145
	catalog-1908475637.xls	Get hash	malicious	Browse	• 199.79.62.12
	catalog-1908475637.xls	Get hash	malicious	Browse	• 199.79.62.12
	INV74321.exe	Get hash	malicious	Browse	• 119.18.54.126
	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 116.206.104.92
	#10052021.exe	Get hash	malicious	Browse	• 116.206.104.66
	shipping docs and BL_pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	PDF.9066721066.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment Advice Note from 10.05.2021 to 608760.exe	Get hash	malicious	Browse	• 208.91.199.224
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 162.222.225.153
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 162.222.225.153
	export of document 555091.xlsm	Get hash	malicious	Browse	• 103.21.58.29
	RFQ-20283H.exe	Get hash	malicious	Browse	• 208.91.198.143
	BTC-2021.exe	Get hash	malicious	Browse	• 208.91.199.225
	invoice 85046.xlsm	Get hash	malicious	Browse	• 103.21.58.29
	copy of invoice 4347.xlsm	Get hash	malicious	Browse	• 103.21.58.29

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
xneeloZA	scan of fax 096859.xlsm	Get hash	malicious	Browse	• 102.130.118.201
	generated payment 330070.xlsm	Get hash	malicious	Browse	• 102.130.118.201
	export of check 684585.xlsm	Get hash	malicious	Browse	• 102.130.118.201
	copy of payment 786442.xlsm	Get hash	malicious	Browse	• 102.130.118.201
	4bedb663_by_Libranalysis.xlsb	Get hash	malicious	Browse	• 169.239.183.80
	viruss.xlsb	Get hash	malicious	Browse	• 169.239.183.80
	9cf2c56e_by_Libranalysis.exe	Get hash	malicious	Browse	• 169.239.182.217
	2f50000.exe	Get hash	malicious	Browse	• 160.119.249.239
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 196.40.109.234
	SecuriteInfo.com.Heur.25915.xlsm	Get hash	malicious	Browse	• 129.232.201.146
	SecuriteInfo.com.Heur.6787.xlsm	Get hash	malicious	Browse	• 129.232.201.146
	SecuriteInfo.com.Heur.6787.xlsm	Get hash	malicious	Browse	• 129.232.201.146
	SecuriteInfo.com.Heur.6787.xlsm	Get hash	malicious	Browse	• 129.232.201.146
	SARS Final Letter of demand. DEFAULTER.exe	Get hash	malicious	Browse	• 102.130.118.207
	yx8DBT3r5r.exe	Get hash	malicious	Browse	• 156.38.154.7
	#Ud83d#Udd0a msgs_jean.ouellette@loto-quebec.com_audio#Ud83d#Udcde.htm	Get hash	malicious	Browse	• 156.38.226.42
	SecuriteInfo.com.Trojan.Kronos.21.31435.exe	Get hash	malicious	Browse	• 102.130.112.81
	SecuriteInfo.com.Trojan.Inject4.8495.10748.exe	Get hash	malicious	Browse	• 196.22.142.232
	SecuriteInfo.com.O97M.Downloader.40352.29588.doc	Get hash	malicious	Browse	• 156.38.221.244
	SecuriteInfo.com.O97M.Downloader.40352.29588.doc	Get hash	malicious	Browse	• 156.38.221.244

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	statistic-482095214.xls	Get hash	malicious	Browse	• 13.224.193.12 • 199.79.62.225
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 13.224.193.12 • 199.79.62.225
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 13.224.193.12 • 199.79.62.225
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 13.224.193.12 • 199.79.62.225
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 13.224.193.12 • 199.79.62.225
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 13.224.193.12 • 199.79.62.225
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 13.224.193.12 • 199.79.62.225
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 13.224.193.12 • 199.79.62.225
	LMNF434.vbs	Get hash	malicious	Browse	• 13.224.193.12 • 199.79.62.225
	SF65G55121E0FE25552.vbs	Get hash	malicious	Browse	• 13.224.193.12 • 199.79.62.225
	catalog-1908475637.xls	Get hash	malicious	Browse	• 13.224.193.12 • 199.79.62.225
	rF27d1O1O2.exe	Get hash	malicious	Browse	• 13.224.193.12 • 199.79.62.225
	cSvu8bTzJU.exe	Get hash	malicious	Browse	• 13.224.193.12 • 199.79.62.225
	Contract_kyrgyzstan_pdf.exe	Get hash	malicious	Browse	• 13.224.193.12 • 199.79.62.225
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 13.224.193.12 • 199.79.62.225
	DHL_988121.exe	Get hash	malicious	Browse	• 13.224.193.12 • 199.79.62.225
	DHL_988121.exe	Get hash	malicious	Browse	• 13.224.193.12 • 199.79.62.225
	SMC PO 1083 SAJ 1946 .exe	Get hash	malicious	Browse	• 13.224.193.12 • 199.79.62.225

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	catalog-949138716.xls	Get hash	malicious	Browse	• 13.224.193.12 • 199.79.62.225
	- FAX ID 74172012198198.htm	Get hash	malicious	Browse	• 13.224.193.12 • 199.79.62.225

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GM DS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 59863 bytes, 1 file
Category:	dropped
Size (bytes):	59863
Entropy (8bit):	**7.99556910241083**
Encrypted:	**true**
SSDEEP:	1536:Gs6cdy9E/ABKQPOrdweEz480zdPMHXNY/gLHfIZN:GNOqOrdDdJPAX1LHA/
MD5:	15775D95513782F99CDFB17E65DFCEB1
SHA1:	6C11F8BEE799B093F9FF4841E31041B081B23388
SHA-256:	477A9559194EDF48848FCE59E05105168745A46BDC0871EA742A2588CA9FBE00
SHA-512:	AC09CE01122D7A837BD70277BADD58FF71D8C5335F8FC599D5E3ED42C8FEE2108DD043BCE562C82BA12A81B9B08BD24B961C0961BF8FD3A0B8341C87483CDE7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....b.....R.i .authroot.stl.qqp.4..CK..8T....c_.d....A.F....m"...AH)-.%.QIR..$t)Kd.-QQ*..~.L.2.L.....sx.}...~....$....yy.A.8;....|.%OV.a0xN....9..C..t.z.,X.....1Qj,.p.E.y..ac`.<.e.c.aZW..B.jy....^]..+)..!...r.X:.O.. ..Y..j.^.8C.....n7R....p!|_.+..<...A.Wt.=. .sV..`.9O...CD./.s.\#.t#..s..Jeiu..B$.....8..(g..tJ....=,...r.d.].xqX4.....g.lF...Mn.y".W.R....K\..P.n._..7.....@pm.. Q....(#.....=.)...1..kC.`.....AP8.A..<....7S.L....S...^.R.).hqS...DK.6.j....u_.0.(4g....!,.L`.....h:.a]?.....J9.\..Ww.....%.....4E.....q.QA.0.M<.&.^*aD.....,.]*....5.....\../ d.F>.V....._.J....".....wI..'..z...j..Ds....Z...[.....N<.d.?<....b.,...n.....;....YK.X..0..Z....?...9.3.+9T.%.I...5.YK.E.V...aD.0...Y../e.7...c..g....A..=.....+..u2..X.~....O....\=...&...U.e...?...z....$.)S..T...r.!?M..;.....r,QH.B <.(t..8s3..u[.N8gL.%...v....f...W.y...cz-.EQ.....c...o..n.....D*.....2.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1492930417120966
Encrypted:	false
SSDEEP:	6:kKu7pkQSN+SkQlPlEGYRMY9z+4KlDA3RUeSKyzkOt:G7phZkPlE99SNxAhUeSKO
MD5:	F6FA9EC53A8143D6336B93A10785A55B

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

SHA1:	018826477EA130220F03F017FE71A8258CB2C697
SHA-256:	E4BECA2475686A264A55574A6B9F751D014420BFA75B7D2006E7352FF6B0D53E
SHA-512:	004DA07660E7DD4D05CCC35D26E471637D79528BAF0BBAE41B8A9E272AE2B2F25FF6DF3D4E9169692FF67B5FCE4168279D7E9E3AE276C996968B840701F0DE4
Malicious:	false
Reputation:	low
Preview:	p..... .....M....G..(..... .....Y5.....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".8.0.f.8.8.3.5.9.3.5.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\10a79fb7-49b3-4c5f-886f-96b85850042f.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	363865
Entropy (8bit):	6.02873300716304
Encrypted:	false
SSDEEP:	6144:ZpubsIwHRYn8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBB:ZAbOxzurRDn9nfNxF4ijZVtilBB
MD5:	6CA6808FDE96951C67013E79D433AA42
SHA1:	04DFAE38FA7FE73B443A12BB597016BD5F892362
SHA-256:	CBF8665EEBFF080501EE7A03996DA19D55B105FE3F3F15080125DEAAE58A6A16
SHA-512:	6D0023295246238A2B91B7F6B371EFB41801CFB0FE586E6F0A9560676C59575C3DF2CF64FD6EAEAE34CA8DBE9D7769DCCEDB437F3768E672B4D075E3E71073A7
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620877810170619e+12,"network":1.62084541e+12,"ticks":116135456.0,"uncertainty":3250639.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132

C:\Users\user\AppData\Local\Google\Chrome\User Data\1b9ca7e9-0400-46f7-9e46-f940759cd685.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	363865
Entropy (8bit):	6.02873300716304
Encrypted:	false
SSDEEP:	6144:ZpubsIwHRYn8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBB:ZAbOxzurRDn9nfNxF4ijZVtilBB
MD5:	6CA6808FDE96951C67013E79D433AA42
SHA1:	04DFAE38FA7FE73B443A12BB597016BD5F892362
SHA-256:	CBF8665EEBFF080501EE7A03996DA19D55B105FE3F3F15080125DEAAE58A6A16
SHA-512:	6D0023295246238A2B91B7F6B371EFB41801CFB0FE586E6F0A9560676C59575C3DF2CF64FD6EAEAE34CA8DBE9D7769DCCEDB437F3768E672B4D075E3E71073A7
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620877810170619e+12,"network":1.62084541e+12,"ticks":116135456.0,"uncertainty":3250639.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132

C:\Users\user\AppData\Local\Google\Chrome\User Data\49ac3a76-2d6b-4f78-843e-69862904ef77.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	359931
Entropy (8bit):	6.015386670858881
Encrypted:	false
SSDEEP:	6144:LpubsIwHRYn8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBB:LAbOxzurRDn9nfNxF4ijZVtilBB
MD5:	ED84A131ADEC636E32A38E4119AB53FF
SHA1:	674CD4E4C07251421334580EEE83896C7619DB49
SHA-256:	5A46AE22E6870C180DEDE5C66EE851FDA7F72584F0FEE9AE42F7AB121E1AE9C0

C:\Users\user\AppData\Local\Google\Chrome\User Data\49ac3a76-2d6b-4f78-843e-69862904ef77.tmp	
SHA-512:	5BA144F0BD69890AB3D559F3ADAC33393E8A0F59EF7231C9731D2C40393E1142483DF48D6BEB97B29192EC69A216367125690EA4D2BB6B0687E084DFE262B63F
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620877810170619e+12,"network":1.62084541e+12,"ticks":116135456.0,"uncertainty":3250639.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7IwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075247322"},"policy":{"last_statistics_update":"132653514054666

C:\Users\user\AppData\Local\Google\Chrome\User Data\5f953a1e-ee68-4646-8309-897945bd7ec6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	363771
Entropy (8bit):	6.028557500863016
Encrypted:	false
SSDEEP:	6144:dpubsIwHRYn8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBB:dAbOxzurRDn9nfNxF4ijZVtilBB
MD5:	9A76DAE83C93BA70926396F092318558
SHA1:	123A0EE03F1BDF5CB81A9889F588471802071AFC
SHA-256:	12D81E5B901F8696CC32AEA266DBB550A3F17472F903738DF7F9E6884507F3DF
SHA-512:	7CF5FB40BB5C4376B6199E96D2E94E6091D08C9E908EB7279D3FB8BB6C7099DB907CF5D71DDA804FA2A45BBEFE2388C96E2A853E47E32A054969D16A8D187BE
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620877810170619e+12,"network":1.62084541e+12,"ticks":116135456.0,"uncertainty":3250639.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7IwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132

C:\Users\user\AppData\Local\Google\Chrome\User Data\7e9765c1-5d3f-4c4f-b7b6-5dbfc3f5b1da.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92068
Entropy (8bit):	3.749217789864233
Encrypted:	false
SSDEEP:	384:nb07Dh+gBRGHCNnrkvTZ30zRgH5QGoHryNXTxktNpsr2rmWhO5HH/AON1PNa1/eb:oKl9KdQIUeL7NdInHOpKL53ko
MD5:	418A36C4CD9989AB7CC7EC4B255EB23C
SHA1:	33F44799E395EAF84691543A800704D173D3CA52
SHA-256:	DF30D985D9EEBDF37151250C5309DCDF677BDBEBA9C5B9B9CFA4528C10E2F937
SHA-512:	E5AED60D014218D659ED3C2D0C53239A3BA48869B174706509D972496D4082FBAD40A02F15CC72F2BE423B511B5461A766ABF7995C5EF8C8BEB84F706D92DC0
Malicious:	false
Reputation:	low
Preview:	.g.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....98.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\88ac6517-9bcc-498d-b42b-c215a914212e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	363614
Entropy (8bit):	6.028199353506257
Encrypted:	false
SSDEEP:	6144:0pubsIwHRYn8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBB:0AbOxzurRDn9nfNxF4ijZVtilBB
MD5:	74A2418E0CD572C1DEF4D1F2109D9CC1
SHA1:	899E849867A9F6534C41CC5AB8AC8B24F40ABADE
SHA-256:	33DB86F0E1C61C00ACA3F03E5A1935523BEFEAA385B444B79F3DBBC09017818D
SHA-512:	0293922C6B46920FE494D91EF38379FC68D6BFABBF697E20E4C993B4C2822BA365F6AFB60EFF6C83FA3E7C17DF06DF452F652D3EADC1646178BC92C632FF3AD7

C:\Users\user\AppData\Local\Google\Chrome\User Data\88ac6517-9bcc-498d-b42b-c215a914212e.tmp	
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620877810170619e+12,"network":1.62084541e+12,"ticks":116135456.0,"uncertainty":3250639.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075247322"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\930ede78-f3a9-4eb3-bfb7-6348e4c2a7df.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94052
Entropy (8bit):	3.7496684793945367
Encrypted:	false
SSDEEP:	384:4b07Dh+g1KR9VKAHCNnrkvTZ30zRgH5QGoHryNXTxktNpsr2rmWhO5HH/AON1PNw:+eKl9KdQIUeL7NdInHOpKL53kB
MD5:	8AFA5AC1EDAEBFCA04B3A6A5EAA4962F
SHA1:	0D6F4208B639F747AB4463D15E39A3B0C5AB64D5
SHA-256:	9444CC5248411F756961A8C7300625A8B8CB6D2C872BFEC1047BEB068CA47529
SHA-512:	1ABFF3D56781BB426B1459E7D22DFD23B30CE33DB739EDECE6DD38ACABA6533FB7FD6F29936AE8A3D3ADB8DCE8DB1D438139D79F50D46FC370715C65170DB17
Malicious:	false
Preview:	`o.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....98.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXYDu6cR9iTXYDu6cR9iTXYDu6cR9n:+Y66cR4TXY66cR4TXY66cR9
MD5:	569FA64ACAA310B1DE1A6250CC7356B0
SHA1:	14251450C245F8612958BF94779E8B72AE6D6213
SHA-256:	AEE20ADEBF2D35EB8A39BE2DC391B0E5966EFCB4AFDC971BB3A18115C929F563
SHA-512:	850914A053EF541046B29260266C17FEFF2466A87784394F9AB3B565D2EA1E656F61F02BDB78F9F9676E90365F837F3709BCC0856B3B844256848F477250E0C7
Malicious:	false
Preview:	sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3020baca-27ad-40a4-888c-a2d42f1de2b5.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22595
Entropy (8bit):	5.535879231409453
Encrypted:	false
SSDEEP:	384:cPVt/Ll6kXb1kXqKf/pUZNCgVLH2HfDLrUJ9HGCBnT2zjf46:GLlBb1kXqKf/pUZNCgVLH2Hf/rUJhGWC
MD5:	DCD8D9E6435BF63907FBB6C61332FDF7
SHA1:	2971460F6C3303EF697A24DB1C2F5AFAA55EE6EB
SHA-256:	EC4340E5C15B98ED178B765CE0762EA2E35AA0DE23957BD86C9DD8B59C5CFBDA
SHA-512:	4BF7A4F8E95BE1FD5F42BA2E427F39D732C59DD0E0403CA47742C7BFDF7B6BD5295C99FF812F037F61FC58D37E49D18C9741E7EC27B3FD7C5BFC0D9650527C0
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13265351406329658","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4fd2613b-1edf-4333-9a79-0ba77e88f48e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	2236
Entropy (8bit):	4.897103102556396
Encrypted:	false
SSDEEP:	48:Y2n6qtwTCXDHz5s4RLsCTsOTTRS6DOsYyKsy3zstMHMYhbxD:JnxOTCXDHznRfT46DaLAG9hVD
MD5:	E243216478C661912C4653AF9DB9A0FD
SHA1:	2943610C70EED21A8F2BE8428EB6B87AE3789848
SHA-256:	8F086941260AF483ACF9781107A40341BF8CE86C5218529D19D3539F4FF3CFDA
SHA-512:	A0E7FEDDCB38BD7AD836449183A1C9171296337D625D1347968ADE40407A088405E2193EF21734210C7A266133CFEE473954CA568DB9A7D99D2F8ED3E543AA6
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13267943411148153","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13267943411198860","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\54683596-35b6-4375-a296-bd9dd18d08b8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5ea0e6f8-9224-475c-9543-23cce0815b5d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6fb72b2b-d8cb-46bb-8f6b-fa4067ebd1c8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	24055
Entropy (8bit):	5.533514116403237
Encrypted:	false
SSDEEP:	384:cPVt/Ll6kXb1kXqKf/pUZNCgVLH2HfDLrUcHGpHGTBnT2zdqf4w:GLlBb1kXqKf/pUZNCgVLH2Hf/rUQGNGb
MD5:	7826EBFC59D8AA8052A976AF8AC2E5CF
SHA1:	8A0FD2B401A0570941CD2A6951DEFFD1863A3CDE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6fb72b2b-d8cb-46bb-8f6b-fa4067ebd1c8.tmp	
SHA-256:	EEC89BE456F20EDF62E5A6F9CE084D5ECD4903D11F75F179B1941B568CFDF5AD
SHA-512:	FB5FE58E3C924401F8AC6E5806BE9443292B71CB717E328B49179E1565787037714154D662F0A2277DEF452B834F4C3D935E1B66BA6FACF9F66EE77EE0716D10
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13265351406329658","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7869e3ea-92be-4ec5-8614-352db34f8436.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5578
Entropy (8bit):	5.166976375622181
Encrypted:	false
SSDEEP:	96:nbrHoe20zdgSVOkIk0JCa/uRWL8xpbOTQVuwn:nbrv2OgSckC4LYE
MD5:	D488E7ED31D14C3F46B0944B4A43C8BB
SHA1:	6F7C52B0797A5F930C585AF3EDFFCCA7E7E5AC04
SHA-256:	3476F96F97B2B0ABD29C915668BBA65FC4EDB595BCCD2D268F0EB6ADC7D78B46
SHA-512:	480EA3CFDCBCBFEA4AF95D4264C71AF75674EDADC697E8AF8FFCB1EAC007792C7D1E1762D1834C9530F775D9A971BC246F929B50C9075E7EBA2054401DC3F CC
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265351407070511","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\79aa9544-d705-4026-a1f8-c9d41e4e2683.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4778
Entropy (8bit):	4.937995835849113
Encrypted:	false
SSDEEP:	48:YcoklSiklqccBqAJbqTlYclQuoTw0uJsM1aPc8C1Nfct/9BhUJo3KhmeSnpNGz0p:nbrvoG2pSVOkIk0JCKL8xpbOTQVuwn
MD5:	359799A06841BC1C1A8DF3828E8358E4
SHA1:	2CA82F2B9E07AAA7DB44DE2E9B8AC7EB8B34FD14
SHA-256:	C6C4872F3EBA79FBD8496D8A014C98E1CBD56B0FA10BD2BE24CB9F027BBCDF27
SHA-512:	61CCDC76D314588FAA8C4C11A10245A991749275FBF5819845CC9C3B9479FCC07F50562C3AF0D0933BDD9600B67CF5C49843AC62AC7DD3E02AA54DC1D4B0D 5
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265351407070511","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.201172013260439
Encrypted:	false
SSDEEP:	6:mXVycZ+q2P923iKKdK9RXXTZIFUtp8VCUkZmwP8VMQtVkwO923iKKdK9RXX5LJ:so7v45Kk7XT2FUtp8sUk/P8BT5L5Kk73
MD5:	B0A3F2CBA005A1DBC330B2FE784183B6
SHA1:	A1FBB1EEB320E5C8DE7DE3E0CFFD38834435CF90
SHA-256:	F8F2BFCE989B50BEC03F3D008BAC6D871BC1A42CD168EFFA0D5D166C3C997F2F
SHA-512:	2BAF9F73A6871F02135D1D3CFE1EC404631DF42F87ECF094D28E523EA0A54DAA99FDF71764D7AA84BB691DE77DAC7057240A672E030CC427BDBEF090266ED2 6
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Preview:	2021/05/12-20:50:24.851 1878 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/05/12-20:50:24.865 1878 Recovering log #3.2021/05/12-20:50:24.866 1878 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.193241843042976
Encrypted:	false
SSDEEP:	6:mXVy6u3+q2P923iKKdKyDZIFUtp8VyhZmwP8VyoVkwO923iKKdKyJLJ:srbv45Kk02FUtp80/P8f5L5KkWJ
MD5:	CC1F87139AB64DC55AD59F1BF7FAE8CB
SHA1:	30DF8D903EA56A0A5B47C9198A177DAE130C65F6
SHA-256:	E92D773462C894113D6AA1ABBC72AF1B84BD989ECC15DBF77C3BB6A48E001499
SHA-512:	6900A68EE8B4665724BA4416AA063CB29B0F407FBA924086AA84B90FD48C0D64CAAD5CADB83CA964F9B81B1348D6D23169A67EAC18A47627305236F8F1C4438
Malicious:	false
Preview:	2021/05/12-20:50:24.713 1878 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/05/12-20:50:24.715 1878 Recovering log #3.2021/05/12-20:50:24.716 1878 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	0.8363502635307629
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmlSHn06UwoEFErr9m:TekLLOpEO5J/Kn7UmFEtm
MD5:	0564E0D13F770ED5CB9256ACB9DBF16E
SHA1:	80FB9EA2B9D926BAE35DF0D91A89B0A11A7C4328
SHA-256:	C065A9F9931DF5C3F74C8879EA4E1194209162D564105EEBD67B19F3AA1F2FFB
SHA-512:	329CDAD97D3146F135965F05F037E07086CABE66B2D611DFAADFDC956BFAF544BFC909C1D23CB812EAC8A13870EE72D9EE39355E94BCB90C14332BBF4130EF42
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9685179778126777
Encrypted:	false
SSDEEP:	24:mIL4rtEy82qLbJLbXaFpEO5bNmlSHn06Uwc8:mI+jq5LLOpEO5J/Kn7U78
MD5:	7283DDA3356B72EB87EEA83B5F6F544F
SHA1:	21E250F9CD260584B8743AD8CD36C8F7EFB17BA7
SHA-256:	A3A30B3E5ED2A053067B65F3C7F3F988359B28FC1BEC6B50122CC399A1F70B3C
SHA-512:	A5A933B5B99449B626198D6E0F1D8B6833C6886971902603B71ED3B12E8D846CF23970149523703E7421216F4BCBC4458198A7F5FF8F066D59E63AA08C8C2E33
Malicious:	false
Preview:	....._O..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2111
Entropy (8bit):	3.80682692186392
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
SSDEEP:	48:34CLb2xec0kK07ZCSZSR07ZzgJgCsTWZahwhlLj/C:34u5ij8hZahQj/C
MD5:	388FA6D67AFDB8F04380C84C598678EE
SHA1:	F67465A73BABCC84BD98C38930D1A5AAD565D466
SHA-256:	54C74F15F2E9FD90D6F5B0E418D545F213D5E21EE4B977EF0DE716F880E3538A
SHA-512:	C6FCC1CF6E4BC25AFCE0C2B0D1B189409C8C1483A9D6544C7607656CEA62F60E9F5ACED2AD4EA9BE52EB77F6F95270B761964FF1794A5C24EA4D41040445130
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...c436de75_e851_4b83_baad_7ae233678d5a.....,.....5..0.....&...{2F4F8386-A58B-4B0C-A17B-2FAAF764E551}.....J...file:///C:/Users/user/Desktop/%23Ud83d%23Udce0Lori's%20Fax%20VM-002.html.....h.....`.....@.....X.....J...f.i.l.e.:././.C.:./.U.s.e.r.s./.a.l.f.o.n.s./.D.e.s.k.t.o.p./.%.2.3.U.d.8.3.d.%.2.3.U.d.c.e.0.L.o.r.i.'.s.%.2.0.F.a.x.%.2.0.V.M.-.0.0.2...h.t.m.l.....8.....0.....8.....J...file:///C:/Users/user/Desktop/%23Ud83d%23Udce0Lori's%20Fax%20VM-00

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	183
Entropy (8bit):	4.267376444120917
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+GgGg:qT5z/t2qoEwhXeLKBt
MD5:	7FA0F874EABF1EED31988230680AD210
SHA1:	E71B360F1E8D5C278A051AD03DFB9027ACCF38C3
SHA-256:	09E15F8939364145E710C314EBD93FD19BF60C2B6B20BF8023315D617B6B141B
SHA-512:	AF4C2E595AA0B1FD96474A0E73530B38BE5F2906B10BE1DEFC0A9221129A3E5BB8D0816777550863AD426C5C836ECA1F0C384986C2A1108E2E4CA20EF10A782
Malicious:	false
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.13064665849572
Encrypted:	false
SSDEEP:	6:mXV6iXMq2P923iKKdK8aPrqIFUtp8V6RQZmwP8V6RjzzkwO923iKKdK8amLJ:sHcv45KkL3FUtp8P/P8W5L5KkQJ
MD5:	1CA4DABA17785C455EAB8CF58451FC09
SHA1:	B373E455FD02DB576381E1DB0B6126FA5A522440
SHA-256:	7E37D3940CE967339EBD63D3B81D3C0ED9E9B04615DC04F5AB1A935DEDEF7761
SHA-512:	B3037C8254FFD34CC69E334B7B00C0C12996C449283845058882EFC2737DB22E36992E5092125817CDB9F19D1E92C32BBCD85277A8CDCE882C28A46FD66A4E1
Malicious:	false
Preview:	2021/05/12-20:50:07.108 1924 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/05/12-20:50:07.111 1924 Recovering log #3.2021/05/12-20:50:07.112 1924 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Size (bytes):	627
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	12:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
MD5:	9D7435EA49A80FDD66E4915F513017F9
SHA1:	469F6C6E4B19B85CC1BE497812B2F20864F4FF2C
SHA-256:	409D4C47E940688527D730B996E8991E010988C7671565467ED69D640D0947F3
SHA-512:	0561CD632D4219AEF4686DE40EC092921384CA89755D354801E0EAEC8645A8630A180807AF518AC8FCF01F71EB3D10FAA9CE1E62C7A7226A274975BDCB7EEB4C
Malicious:	false
Preview:	.f.5................f.5..............f.5................f.5................f.5................f.5................f.5................f.5................f.5..............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.118269746811279
Encrypted:	false
SSDEEP:	6:mXVEKXMq2P923iKKdK8NIFUtp8VERZmwP8VE3yzkwO923iKKdK8+eLJ:slXMv45KkpFUtp8K/P87z5L5KkqJ
MD5:	C33297D9A04DEAB2F4285C5E023481DF
SHA1:	15D359EB3FDA90447F47E3DB3BC186BF0D22A116
SHA-256:	C87AE5C27C75199199250939EF6D31460999E3B1EFF7FAD265FB45BD1A39AC48
SHA-512:	43D682D80FCEBFFDD26483B9E285AF74ABEF8B71B30C06F78520F8FEF8EEC0CE1C6F97EDADE7AA9335534902CF3A840EF95D43A31C4C3F803F7C7F2134337CBE
Malicious:	false
Preview:	2021/05/12-20:50:10.443 1924 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/05/12-20:50:10.444 1924 Recovering log #3.2021/05/12-20:50:10.445 1924 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_1_metadata\computed_hashes.json	
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.9308383808090301
Encrypted:	false
SSDEEP:	48:yBmw6fUyrBJgC2/wb/w07oJnw1Ok02TXUBdsxxelJgCi/wf/B07rBu:yBCRrBw/8/cJwsn2Tkvuelw/6/2u
MD5:	75EEC6330450EC284305E967612029B2
SHA1:	920010508DACE4202873F39A09881A8C5CA044DF
SHA-256:	AC589FECC5F7B07A917A188B1E82E5568BC406289A948E505C77C167F2F175D9
SHA-512:	4C41FE839A6DD8F53FC6ACF5031061548666DCA759139E79499B3B1A149902461538CC0FC30E9C2AB6AAE9221B0472716CDEA54B08DC2258E6209908C4966338
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.7759188720324741
Encrypted:	false
SSDEEP:	24:VKVSyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6Uwdt3n:VKVSdBmw6fUkt3n
MD5:	362F7A094F6C6279D4F0366F10FAB62B
SHA1:	ED9CEB2B781AF9356E5753CA87D7AB777D0B30E5
SHA-256:	D82D21D6109BA376D8B93073346007B419C50E7FAFD759E92C07306E118B2095
SHA-512:	F4A0533B2E6B208C1794E60DB564D2842776EA00C129AF52E23D095B963365BCA94332EC22557E2FB67409072367900CF79231DE77875110B7ADD7D183BED1C1
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Preview:	.....+L..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	374
Entropy (8bit):	5.232984248345586
Encrypted:	false
SSDEEP:	6:mXVw9+q2P923iKKdK25+Xqx8chI+IFUtp8VwwukZmwP8VweQtVkwO923iKKdK25N:sC4v45KkTXfchI3FUtp8Ca/P8CeQT5Lk
MD5:	7DCB1977F51CA748C8908B12573F40A8
SHA1:	D7435A0C13D255B6898331E74FE5CB66404D157D
SHA-256:	B84A3B9A8633D876776B5618CCC6A6F3ECA097C6C38812052FEE0ABFD1606D3D
SHA-512:	6BC9A1FF0B842BA67D5094DFB93BE53EE736028DB30E0F0A96B9832F4ACE4D0CCBF8A548C3EE062A57CBCC4F1977F72A744E3A3C32CF42525FCDEDD5133EC C97
Malicious:	false
Preview:	2021/05/12-20:50:24.542 1878 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MA NIFEST-000001.2021/05/12-20:50:24.543 1878 Recovering log #3.2021/05/12-20:50:24.544 1878 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	360
Entropy (8bit):	5.191645320814612
Encrypted:	false
SSDEEP:	6:mXVwn+q2P923iKKdK25+XuoIFUtp8Vw0ZmwP8VwbVkwO923iKKdK25+XuxWLJ:sC+v45KkTXYFUtp8C0/P8CB5L5KkTXHJ
MD5:	BC74FA46E850ED5848D4AD307433CBFC
SHA1:	9B4AED329DD3BF9FA99B166ECAB087FA5744AB7A
SHA-256:	AA9692C408AE34E05C50D824CD0D64C9952C7355D6D2F2FEFADE0F1A262AFBDD
SHA-512:	C945050EF3C49A318848A3D9C0E122DE6E1E083E4ED7EE9FEDD1E50539F7614922364A7C66A7D9C83641A8A6DCA80F8D4CA635C3CC296BD225A1B203D50165 F
Malicious:	false
Preview:	2021/05/12-20:50:24.531 1878 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/05/12-20:50:24.534 1878 Recovering log #3.2021/05/12-20:50:24.535 1878 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.1796344931071125
Encrypted:	false
SSDEEP:	6:mXV0smSVq2P923iKKdKWT5g1IdqIFUtp8VjYgZmwP8VmAJIkwO923iKKdKWT5g1L:sGsmOv45Kkg5gSRFUtp8hh/P8sL5L5Kg

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
MD5:	68E424063700021E2317BBE1EB8AD7B8
SHA1:	6BD4A5231EAA98009709B4EF971DE40C66C6159E
SHA-256:	79C2C9FDA5793C81EB38CF427B15011761190C424F75B20FEF616840EF15365F
SHA-512:	97AB0B0B57F4D2DB6BFD6BF954584C422AB4C249D06333619F1771970E84096AE541C28952F4C00AD0F1A730C5C61B4B0B6B973F19AA16AA2560FCD938884DB
Malicious:	false
Preview:	2021/05/12-20:50:24.119 1870 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/05/12-20:50:24.220 1870 Recovering log #3.2021/05/12-20:50:24.234 1870 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.5088678144952523
Encrypted:	false
SSDEEP:	48:TQ/wWJgC4307YS/+/UgjgLJgCcr/e/wP07J:c//yTS/+cgCyr/e/T
MD5:	A84CCB8F9E038F28C4BF6C0FA5191B7D
SHA1:	3F34868D522D290128489DADB86DC601E159EB29
SHA-256:	10ECD8B36248DC5881FE57B363E3C77E455C43779859F315F45C97FA2C43874B
SHA-512:	9EB792AA7EF438BCDFC2A60EDD03B779B17C4F9E97F7A72DF30923839463B394269E739AB3A3826BC62E56FE21C67439C93243786EDDE6F52C88963B39D199B
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2381
Entropy (8bit):	6.015760445354866
Encrypted:	false
SSDEEP:	48:wRSgCaJD9mSgCL2ME2bI/Ch+a8Br8/UhTG8jHj1AyVw9XjJgCH/wT207G/UiqM:wvJDv2MbUUihBjiyKjh/J/ULM
MD5:	F6DF103EAD0ACD9F717E94BF49331C85
SHA1:	9C335E8119C6CD39C70C2154A88BA655F58F9CE3
SHA-256:	E6175308BA024AD03A66210F65DC41C9CB12BE67A5AFF65BA338BF34BBC3D4A1
SHA-512:	8BD8C00F7AB280BF346B1C36DC7E064CA32117AF3E5A6272A5971A927C4424A7955218719507043F14A4083F1A14DF14947BD490466A60C49CD8F4A6842BF1F7
Malicious:	false
Preview:	."......account..bg9yaubjyxzhlmnvbq..com..https..phfax..raghadstayl..signin..to..todwll..your.laphcdnjr38g21buqsiwfemok6vyz9t540l7xdfyz3h15mti2cb8x4el967wvsja0nuqkogprxl3wvneaqy5izj0ckrftpsu7m9h218d46bgo..data..cava..cd..co..doreenbrown..lori..tele..za..002..user..c..desktop..fax..file..html..ud83d..udce0lori's..users..vm*.....002.....account.....user...p.laphcdnjr38g21buqsiwfemok6vyz9t540l7xdfyz3h15mti2cb8x4el967wvsja0nuqkogprxl3wvneaqy5izj0ckrftpsu7m9h218d46bgo.....bg9yaubjyxzhlmnvbq.....c.....cava.....cd.....co.....com.....data.....desktop.....doreenbrown.....fax.....file.....html.....https.....lori.....phfax.....raghadstayl.....signin.....tele...to.....todwll.....ud83d.....udce0lori's.....users.....vm.....your.....za..2...%....'.....0.....1.....2.....3.....4.....5.....6.....7.....8.....9.....a.....b..c.....d.....e.....f.....g.....h.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	42076
Entropy (8bit):	0.0902328517903178
Encrypted:	false
SSDEEP:	6:NllqellKlltl/9ll3TllujlldTllkll/vg9bNFlEwtCS/lnaKl3lXs75fOnd0XiA:EDgh4vqLipS/dn3lXs75fOd0S9Lu
MD5:	C9E6506D37EEB33719E6E04ABC46804C
SHA1:	66111F8B0AF7D42463AC5AE2A954202003B0B06F
SHA-256:	C8C745C927B09C8DE1A5103A7FAB87DB707C68701EBCB1E6C9D18F82203B0210
SHA-512:	F215E9D1691B146A9F338B061BF4F080AC33D2AA98BC4DA047845581DA7EE1901F5F5F958006FA7F1220DE4542639FF3EFD399AC961A5ACAB76E3553D07C4DF
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.466491051244718
Encrypted:	false
SSDEEP:	48:d1GVxa7dMg8dbP9N5bQSefgG6NrS0U9RdiN9L:ka7dMbdbP9N5bQ5fgGmrS0h
MD5:	1349E765F4E9713BBA8B39BF2AB999E9
SHA1:	E2451E6ACC0FE726A56213C652E6F5BC2E294184
SHA-256:	4ED903A4CE3F5409D2036D162BD0A45739DD95C03628A12BF07D8CC108AEF2EC
SHA-512:	865E87DB9C9DDCF91BD656D1E123B5C3D3831BD9F387C5C45FA40644DE608DE47B956D12CF7677F104FBC222758600933ED3501BC11D5B0A20200B3A7110275
Malicious:	false
Preview:	]..''...*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..776210000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-05-12 20:50:26.31][INFO][mr.Init] MR instance ID: 04c247e3-97c8-49ac-b4b4-374cf130c3a5\n","[2021-05-12 20:50:26.31][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-05-12 20:50:26.31][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-05-12 20:50:26.31][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-05-12 20:50:26.31][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-05-12 20:50:26.31][INFO][mr.CastProvider] Query enabled: true\n","[2021-05-12 20:50:26.31][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.156135015540778
Encrypted:	false
SSDEEP:	6:mXVP6L+q2P923iKKdK8a2jMGIFUtp8VPd3Fz1ZmwP8VPllLVkwO923iKKdK8a2jz:s4L+v45Kk8EFUtp8pZ/P8/lLV5L5Kk8N
MD5:	B817FCC04A1ABB2DC674C062C5D2EF19
SHA1:	233026F4F26091D580664755FF6F65C0869F5392
SHA-256:	FEFBE39ACF8E55F1F950A6740F06F2AE0820BC4560780C6B148B4B5C0AB5BC5C
SHA-512:	2C0D18257DD2A92B91769E6C8DA6FAE424A38841C7346CBFA031FD0C4C194492AB1E454CD4477D2FDD951B60A3F15DA884F8E49B82B54F90EB2E22506020885
Malicious:	false
Preview:	2021/05/12-20:50:06.231 189c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/05/12-20:50:06.234 189c Recovering log #3.2021/05/12-20:50:06.236 189c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.145292600525004
Encrypted:	false
SSDEEP:	6:mXV6ZBIq2P923iKKdKgXz4rRIFUtp8V6ZFFZZmwP8V6ZqkwO923iKKdKgXz4q8LJ:sRv45KkgXiuFUtp8i/P8/5L5KkgX2J
MD5:	99BC2EC18611338E4989ECF6DA87D8E8
SHA1:	8F03DDA9B745A5E1AFF0C8F57172252859A7A9E0
SHA-256:	C3AAD08FFB8571B3FF6D4F0D7F9801538EF22643429FAA8DCD6FECFE9B8E1F61
SHA-512:	465D25C6BCBF3F23889D1E923602974E5AE6EDCD380445B5C6D2CDB8FC5E95C3FBF21E133E09C0F9C8F5966B4E33F91E6A0281B1A8E263A7107F8750849294C
Malicious:	false
Preview:	2021/05/12-20:50:07.190 1924 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/05/12-20:50:07.192 1924 Recovering log #3.2021/05/12-20:50:07.193 1924 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.0112756919450352
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUOoTRs2oTRsAoD:wIElwQF8mpcSJ2Yn1
MD5:	741C76CF8C946B15CD9EC92F13D3CB53
SHA1:	C6013C90B18D8371EC7006AA6A554DD260738F41
SHA-256:	A6365666874B615C0161A82D90236D643C0C00E902EDBD083A738215211073F0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
SHA-512:	DA80C4C56E4C885FB89B189EDB234E2C9ADBE7B39BA72209168D1E9CDAFCE3656171C44225F314D6654EC0943F86C364C77E27628EF59A5F926A6AAA7005470
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g...^.....j..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	21044
Entropy (8bit):	0.8206353331879722
Encrypted:	false
SSDEEP:	48:TYqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUe6:TYhIElwQF8mpcSH
MD5:	34940A7C6151D8048D97C401A4959930
SHA1:	A8F30D2E2ECB8B67D4A2CC32AA902C58AF8EEF36
SHA-256:	A5E9051CD1F4C2F2994ADC6F2CDB409E0E03FDD220B0135CC47DF511065CA055
SHA-512:	1F723B0497179AC52E9C9E4A25985B7B1AB95B02FE7FD4BF0243E529E6670F8E2082FF941BDE2859477349D9F5E5A95ABF195222323830EAD99A54FA61169EC1
Malicious:	false
Preview:	.....i..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljl:5ljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.083288936916014
Encrypted:	false
SSDEEP:	6:mXV6dlyq2P923iKKdKrQMxIFUtp8V6O1ZmwP8V6YRkwO923iKKdKrQMFLJ:s6lyv45KkCFUtp8R/P8NR5L5KktJ
MD5:	57DE72CE4C9062581105001BD38B21D5
SHA1:	394065F7297EDB06A251F9DA7A3407C8BA6F64B1
SHA-256:	3696446C8266462E0B694774838F0B7BAD11D575E7E307776F911000DEDFDC2E
SHA-512:	FF934A5F9E04B94324793BDDDD4E6F84C08FCE1C33EFD5F886177D12283D8F894151E3891B5DFA9EB71C6CC9F19FF8584C958311B017DB1705F8A17464D11E6
Malicious:	false
Preview:	2021/05/12-20:50:07.038 1930 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/05/12-20:50:07.040 1930 Recovering log #3.2021/05/12-20:50:07.040 1930 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	350
Entropy (8bit):	5.141592628943145

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Encrypted:	false
SSDEEP:	6:mXVPxQL+q2P923iKKdK7Uh2ghZIFUtp8VP3SG1ZmwP8VPOQLVkwO923iKKdK7Uh9:sQyv45KkIhHh2FUtp8d/P8tR5L5KkIh9
MD5:	9F1DA8F82D46520EFE9C87331D0F7FA8
SHA1:	61F50DBB247368036D77F41686ECB803386EE9BA
SHA-256:	B8080AD7837F21BF1FB9B1AF0CDCEEAD0BDFA55FA0C45E9F99214C0D7F9CA3C3
SHA-512:	52AB3D017F1082389DF6F486EB2FEBE02E1DAAE0E43DEA87910901BEB2FE124F197380C717C7716C8F9C2517AE16DC100C650810738C82B8EF0E4CB294FF1E7
Malicious:	false
Preview:	2021/05/12-20:50:06.072 1898 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/05/12-20:50:06.075 1898 Recovering log #3.2021/05/12-20:50:06.079 1898 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site C haracteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\4d68cbbb-c5c6-4205-b99f-92b08a650e3e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","port":443,"protocol_str":"quic"}],"isol ation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Preview:	.'..(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.193329552268295
Encrypted:	false
SSDEEP:	6:mXV6Lgyq2P923iKKdKusNpV/2jMGIFUtp8V6RBvz1ZmwP8V6Rj6RkwO923iKKdKK:sxyv45KkFFUtp8U/P8JR5L5KkOJ
MD5:	55CFBF59F62A38EBC7BD7B82C8595571
SHA1:	4BC5CC175EFC13D9B2C81C9AC11D62B4EAA00BAC
SHA-256:	E34C737D9D963CC4DDA9D06299838119728F28A9CA5C4CEE534CB7903A3732B0
SHA-512:	791B852F254B8FDDB43691E644AEBC0090FEF870A0D3404306C9DD590A774C2409E9EA808BD93C29F70E2D70EF38282946AAF267B2AD1925CD06B0883304C797
Malicious:	false
Preview:	2021/05/12-20:50:07.109 1930 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/05/12-20:50:07.111 1930 Recovering log #3.2021/05/12-20:50:07.112 1930 Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Category:	dropped
Size (bytes):	434
Entropy (8bit):	5.243146713030311
Encrypted:	false
SSDEEP:	6:mXV6ZGyq2P923iKKdKusNpqz4rRIFUtp8V6ZBWr1ZmwP8V6ZBW9RkwO923iKKdKr:sRyv45KkmiuFUtp8WS/P8W6R5L5Kkm2J
MD5:	53C05E643EF6892A5971CB2E26ED768A
SHA1:	76FCB937CDBE26CCC1385EA6AE8F85FFAF072BC5
SHA-256:	0A7CC697DF12153C531AC9CCC7FAB1480ACD3E408A4FB3F2250828E650F514C2
SHA-512:	8EDB7CD16F0F7275CB3812066059F181C4DCAB85F9624F012760C58391E0DFC18E92F589A6C030939633B3A0AE491537932483E26CF58186644A9EA22CF26815
Malicious:	false
Preview:	2021/05/12-20:50:07.192 1930 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/05/12-20:50:07.194 1930 Recovering log #3.2021/05/12-20:50:07.194 1930 Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.26128381655407
Encrypted:	false
SSDEEP:	12:syM2L+v45KkMFUtp8yd/P8yLElLV5L5KkTJ:q45KkUgwlL5Kkl
MD5:	51E0D63453F1FB711D2D5AE96F0FEA37
SHA1:	CCD2FA396A2945C60E44C4828B1B709DD2E9F77D
SHA-256:	7E9443CC753E179EC54C69BB776BD7E6B2BC3AFCE4741E11379DF5E4DB19C02F
SHA-512:	F7F6CE790AC2314599C31593FCC65A0B6BAFF9A21F1C3EBB8D93B93F0115F0F315137EEDA6CB18AF2D5716E34E6E3E6F5584C7DCF158594F6C4DE04B664AB6A 7
Malicious:	false
Preview:	2021/05/12-20:50:27.261 189c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/05/12-20:50:27.263 189c Recovering log #3.2021/05/12-20:50:27.264 189c Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\2c9daf34-360e-47e3-bd47-7cb8fb610dda.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.976576189225149
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5OV/sDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdysBdLJlyH7E4f3K33y
MD5:	5886A009EB58EE06A16EFD6D1BA9A046
SHA1:	A867B5052F3FBB811693DF8CE3FDAA794F2F2E40
SHA-256:	9E3392126DE2D81D019E0AB3E17F20BADD0EC9FBD944BCB7C4DAF449D937D496
SHA-512:	D24F30A2E35F903AC10AACC4425C58BECB1C6BE2BA30A3C2B9D9D46CE04914AA71F55B3B16ED89081AD65A7090C77F5DC4A258B7B98D71E6A994D176536FBI 27
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542597817103","port":443,"protocol_str":"quic"}],"isol ation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	592
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E8E:8N
MD5:	B505641E5E90B7CF4BC869DD1B4BE451
SHA1:	0EC7B13DC043E054AB48B8F45FE49EF1209C01AA
SHA-256:	2755F85F14CF33404CEEBF053D0CB79DC3B98D643A51075737E6A5BE154FE1D9
SHA-512:	610AF095630C93B0586F4D9CA84FA75454C472C557D4FDBC0D5C1851F9AABF8653079A7ADE4659ABADDEDC2E02E58AD13C7244CD004B0AA5A462307F293F833
Malicious:	false
Preview:	.'..(.....'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.169699146339516
Encrypted:	false
SSDEEP:	12:sMQ+v45KkkGHArBFUtp8OdW/P81QV5L5KkkGHAryJ:t45KkkGgPgkL5KkkGga
MD5:	FC933BADEE1FEE6D5EF782FF3A3CDC4A
SHA1:	F3487C1C4DB0773B19D3FC1697E7323D723121C1
SHA-256:	ACF3DF6D1598671AA5166DE6F236466DD59419C0264EC2EB8EDAF318B7404098
SHA-512:	FFC09CDAD48A7DD5F7E26F8113A4260FFB5D2A965C1F804B34C076FC78C9F90900E2640200E0673C7E44FE9FCA1A453FA3220E5D51A2EE893A674ECF2B90130
Malicious:	false
Preview:	2021/05/12-20:50:24.343 193c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/05/12-20:50:24.349 193c Recovering log #3.2021/05/12-20:50:24.351 193c Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	434
Entropy (8bit):	5.198863775041036
Encrypted:	false
SSDEEP:	12:sdlL+v45KkkGHArqiuFUtp8BZX/P8SLV5L5KkkGHArq2J:G645KkkGgCg8HL5KkkGg7
MD5:	265174179E6130B3541EB660FB276F39
SHA1:	9100D331B091500C62212982AAE900BD3B46098A
SHA-256:	8C3F617F057E1FF1815D2E66A51B51459482D45BE45944C41BA370C61CABE753
SHA-512:	489EF413985F6CC32156FC2CBA0726C5557CEAD01CB8DB2CD52478C28A0EEAD3EC51A6FB5ED3E7C32058A8AF6C94DE8694F62EBAA3A13C4577C6C8AC424DI 43D
Malicious:	false
Preview:	2021/05/12-20:50:24.344 189c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/05/12-20:50:24.348 189c Recovering log #3.2021/05/12-20:50:24.350 189c Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljl:5ljl
MD5:	E9C694B34731BF91073CF432768A9C44
SHA1:	861F5A99AD9EF017106CA6826EFE42413CDA1A0E
SHA-256:	01C766E2C0228436212045FA98D970A0AD1F1F73ABAA6A26E97C6639A4950D85
SHA-512:	2A359571C4326559459C881CBA4FF4FA9F312F6A7C2955B120B907430B700EA6FD42A48FBB3CC9F0CA2950D114DF036D1BB3B0618D137A36EBAAA17092FE5F0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Malicious:	false
Preview:	..&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.182538904693017
Encrypted:	false
SSDEEP:	12:sbEL+v45KkkGHArAFUtp8bGY/P8b6LV5L5KkkGHArfJ:El45KkkGgkgSWIL5KkkGgV
MD5:	5B471DCBE63B75086360443F6B91C7A4
SHA1:	4EA2A17191F866AE120A32ADCA341DA04388026F
SHA-256:	93AA05434DE97815750A7A1066E46A04B4707C6AD901C8F5656D92B180B9E4A2
SHA-512:	1908FECCE642B2CB2AEDEFC7F83B397377FD6007F0EBF14D7DF1847D1670136FFB47CC345DA7FAC636D064571C4A8499F6E83CEB6B73988E609086B06E4FF75F
Malicious:	false
Preview:	2021/05/12-20:50:39.651 189c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/05/12-20:50:39.652 189c Recovering log #3.2021/05/12-20:50:39.653 189c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.213351521698195
Encrypted:	false
SSDEEP:	6:mXVPUpFlL+q2P923iKKdKpIFUtp8VPUVz1ZmwP8VPUgLVkwO923iKKdKa/WLJ:silL+v45KkmFUtp80Z/P87LV5L5KkaUJ
MD5:	A7BA12AFF9B0215970A3F66CD0765CB0
SHA1:	FAE997ECF39634D51D66ED4EFCB7C4B477EB08A1
SHA-256:	5E4EEB97CDC8512208D8C1161162D36C119A1402F1223A9CE1A9FF971F780737
SHA-512:	157643331F5F8BF653E1DE62EB5861C5C493A4101E1B4EB99B6B5D4BCF86C6ACABBE05793F1B9CE436084CE5A4CF5881D21FD78E822638BBFA2BE1242904040A
Malicious:	false
Preview:	2021/05/12-20:50:06.134 189c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/05/12-20:50:06.136 189c Recovering log #3.2021/05/12-20:50:06.137 189c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.281576897222519
Encrypted:	false
SSDEEP:	12:sOL+v45KkkOrsFUtp8T/P8iLV5L5KkkOrzJ:Y45Kk+g8L5Kkn
MD5:	CFCAF50A3B3B7EAE300C0409494156CB

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
SHA1:	A3FCF152A580C6686EDA6010F243BA01898FDA6C
SHA-256:	41BF30A6923DAF633BACA23A36C94E0180595611053A79A0B7F5EF7522042BA6
SHA-512:	7B697C1EA99891767829AF18230DC942DC2D2929721AC71EB4A98E9DE0C7890FEADF300CFE4325C4925761B5B62F24C406FE2B8439026EDB8F775C54CE56A7E
Malicious:	false
Preview:	2021/05/12-20:50:26.309 189c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/05/12-20:50:26.311 189c Recovering log #3.2021/05/12-20:50:26.312 189c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.896834613373054
Encrypted:	false
SSDEEP:	3:/uArRt/1YBgMErOjn:/uArRt/a2MD
MD5:	E1CD9BFD7F17B1E253CE9D0A1770FB04
SHA1:	FC32C063BB9967F501EC95C55B62B50E4639CDF7
SHA-256:	798D4ECB74A4EBD7EDB4E4C3E61205D69D722E5EDCF9AB9D79B075B108157BBE
SHA-512:	509A1C6FF0CA6DD60191073C1B8BDB93CDF1E0700053D12F8FE26D7C3ED0A7FD4DE466CDE12C6761FA2962FD93C669C9A5063BD725ABBDCB1D6463D71724290
Malicious:	false
Preview:	.....G.....L.P_..F.....P.....&Viu.....x.k...X

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\0c5b87c3-5d83-418a-8a7c-726f230d87da.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	175509
Entropy (8bit):	5.489440694064333
Encrypted:	false
SSDEEP:	1536:rKbsLAR2A4VBQV1111111111111Nr366R6faFR+up0y0y2im1OsFcgYzQNL9X:rKbsLAR2fe/FZntrslfX
MD5:	33EABC19FDF40F3D36B6870EF5861957
SHA1:	CF3EF59C3940B58C314E9F6A1616751553F2D9A2
SHA-256:	647D07F37554672865902B2CEE80864B5A5283C372C7263BB1497D5582054E57
SHA-512:	47CFEDB1FDBC9BC09905C70F69A5114C64A8FC791BCA480D24972275276F00CEB230C579B4217337F9C69ECB2AB3221A3B549F06E8074D76BCE2F31773FB69F
Malicious:	false
Preview:	..... .H..... ..... .p..... .h...n..... ....n...((.... .h.....00.... ..%..~H..@@.... .(B..&n..``.... .....N..... .(....D..... .w`...M..(..... .....+.O-8&]P>/^Q?-^&:?I.1;<....qye.f.%.....X...E....I...k}....{.m.t.CP.....E...\.....=H..,A..,J..;P.....nn p}nnp}.....~~~.....!...!---2---2.. .....(..... .....!...7.#.:3,";3,!<.&'/.....NPLYt.F.K.%.....L..C.....1...`...KOPVutz}..A.BxX.....P.. .Q.....1...x...tqpyxuux...0D..DP.....G.....uojuppnw....t|..9F..-=..+:..5:..rr.....llkrkkmw.....ggitllkv.....hhgssss~.....YY\eYY[e..... ....nnnzXXXa.....RRR\.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16
Entropy (8bit):	4.0
Encrypted:	false
SSDEEP:	3:SeFcn:Sec
MD5:	61B979ECA159ECAC9C7F8F1D6FD43E9D
SHA1:	0373696351FC2172E811DA8393DEC84036FA34A0
SHA-256:	AB05E0A6FF7E8FFF89F924B279D93AFC72ACCE817C4D250C60BB8059CC534303
SHA-512:	C95825DA33CBDDFA627D9FF9A5B8371BC5F4E643A09573B6E1E839A83B619F53D878C344030B9701DCBC24D4CECCC016CF4D298D10EE8C37D1B5FEC1A5168B6
Malicious:	false
Preview:	F.....r...(R..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a1e6d5f0-8f54-45bf-afb8-f5c7c4c938f8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a1e6d5f0-8f54-45bf-afb8-f5c7c4c938f8.tmp	
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.535960531700453
Encrypted:	false
SSDEEP:	384:cPVt/Ll6kXb1kXqKf/pUZNCgVLH2HfDLrUJ9HGpBnT2zuf4Z:GLlBb1kXqKf/pUZNCgVLH2Hf/rUJhGT6
MD5:	53EA7EDC8467EA125F93C62B66647C5F
SHA1:	F78B9FBEB1E3FA8A602080605C1B9B9AD16DD891
SHA-256:	23C776A586971FFD61AE6225B94E4F7484754EA2CF40D7EB7A8535CEDD7F1F12
SHA-512:	4B559F0E68BBD7F3474296112C81FF964180D16E6EB931E5B4073AE489510A7A916A5F0B16870E3B5AE04EC60F5D363217DAA27879E7546AFA09B80BC0EB0BA7
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13265351406329658","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b01d0f88-9fb0-49a9-8712-81b53b9c9d76.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.577596370028223
Encrypted:	false
SSDEEP:	384:cPVt6Ll6kXb1kXqKf/pUZNCgVLH2HfDLrU4Hf4PW:RLlBb1kXqKf/pUZNCgVLH2Hf/rUcft
MD5:	2EAA96E7458E0AA4AC130F971860C685
SHA1:	653C164793EB69FC0766B994C8807EECCF5A0AA9
SHA-256:	60304B95363ECDE853D27B538535FC76BEDF30BB4BF4FB6C32CEDCB61FDB44D7
SHA-512:	3F279C1A01369E1216FBF2FE133029A61AC65EEFD94E91AB4EBBBF7B007C419FB17D2186B12D9C59B4A77C7D8E0773B06EDBCF611533C48CF16D21CF5693654E
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13265351406329658","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cc96df0a-b138-4980-a4ac-48b1f7fd88b5.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5668
Entropy (8bit):	5.170596583075726
Encrypted:	false
SSDEEP:	96:nbrH5e20zdgSVOkIk0JCa/uRWL8xLbOTQVuwn:nbro2OgSckC4LYa
MD5:	9D108980308BEE61D7DD7440DC5BBC5F
SHA1:	CFAC7097D3D98F0C9F8C71EEC977876F6A3F7B5C
SHA-256:	D03356A2EE14145A81B0FB268D0BFA31E83519F3121DCB00237D99395FB31A26
SHA-512:	5E808E395E7E4B595FBC44B9D0B01E28D0318FCD63906DCB8D40500DD77E259B3F8DE938D6936F40BC860211875197C32A301F41F09495BEBC44727372CC75C
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265351407070511","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d5b45935-62c7-4afb-8b2b-5a446b246f56.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	874
Entropy (8bit):	5.550136371265034
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d5b45935-62c7-4afb-8b2b-5a446b246f56.tmp	
SSDEEP:	24:YT6H0UhHPkG1KUe9aUeCcz7wUBEKRUeIQ:YT6UUhvDKUeAUeCiwU9Ueh
MD5:	7F1C38F13260D27C390C3BFE490F0B1B
SHA1:	C96BFD1CE1BBD3940D4FAF5678B8B7DC429F9443
SHA-256:	ED766478E8BE7CBD062EAD632BD9B27F0C18FC47B543EB69525C449E15FA8306
SHA-512:	CF2542CBA979EDBAC1317DDA3ECA13C12B07100A0DF1E09478BECDA1CDD583620D4A75BAF9BBB6EC07A3C99CD046C4785EFE2ECDF658A3E055083CACB0B C41C
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains" :true,"sts_observed":1601477028.822838},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_in clude_subdomains":false,"sts_observed":1601477028.743728},{"expiry":1633013040.850112,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=", "mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477040.850115},{"expiry":1652413811.148309,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C 5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620877811.148312},{"expiry":1633013028.952627,"host":"+ccWXqaoHJ 9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.95263}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.376602566012997
Encrypted:	false
SSDEEP:	3:tUKCgQUljmSgZmwv38gQUkVH7W01V8s8gQUkVH7W01WGv:mXVUVJgZmwP8VUkRbVv8VUkRbtv
MD5:	8F45B33A987EE19894DBB258B5E325B1
SHA1:	78B583059F9B43BB4B6945AA7EDFD016910029DD
SHA-256:	680A7D9DFBDAF4005199F76B01E0E95A4FBB49C2A96D71F7ED9558EE12BD7262
SHA-512:	3275B394643772EB4CAE2A33CBDB047BB7AF6397DF839A9B34D7BCCA572A2EF47767B8000844F6728CD6D73014157D591E0F8BF94179C8176F6CF2F97EA6EBC
Malicious:	false
Preview:	2021/05/12-20:50:23.414 1870 Recovering log #3.2021/05/12-20:50:23.508 1870 Delete type=0 #3.2021/05/12-20:50:23.508 1870 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF 04
Malicious:	false
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Category:	dropped
Size (bytes):	340
Entropy (8bit):	5.162250276756089
Encrypted:	false
SSDEEP:	6:mXVSE+q2P923iKKdKfrzAdIFUtp8VSnqXZmwP8VS7NVkwO923iKKdKfrzILJ:s0v45Kk9FUtp8nX/P8Yz5L5Kk2J
MD5:	7FD53B7878F26CCDB1C84455C84A12A7
SHA1:	D4211A2EFB3AA29FE6F2593F5CEF3C24B08F6680
SHA-256:	0EE8DB992AF49D2BF5B6AE5C2069BB86CB904EBB79BB87E5AB98923A7CAA2CC7
SHA-512:	E98DBB8E4EDE14FA4DB0AD34AF6E9AE0DE7A7B2B1477D002FBBCF81237FD880FD07068CA19A1DF25EC5F9829A106896886073D4316D6E7EBC78B53471633B7AE
Malicious:	false
Preview:	2021/05/12-20:50:25.104 1928 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/05/12-20:50:25.106 1928 Recovering log #3.2021/05/12-20:50:25.107 1928 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8150724101159437
Encrypted:	false
SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4
Malicious:	false
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\9.22.0\Indexing in Progress	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir1700_906835169\Ruleset Data	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir1700_906835169\Ruleset Data

Category:	dropped
Size (bytes):	208920
Entropy (8bit):	4.964307261909652
Encrypted:	false
SSDEEP:	3072:gzChBJeloN++/mYWcT8WSkb1RqmYb8zpoPo/smfgbpxT0C0oUBXrvzpnuidAut:5clEHRAqggCylW1
MD5:	A96F63877D2B8648563905C60513B9F0
SHA1:	EE63F5F68E176DCEA8416C9877F09533C4E5498E
SHA-256:	B5A3D515B1673D134B197878D681C0CC8290BC476EB69D69EF27FF9669EC2E80
SHA-512:	C137035D92E4161FF55AF447D61F7F61E9FB8812EF0D32649011A6D7A07AEBA317B4197CF0205B37B755FACF7A1ABCA586507A1B825BC2FD4194E8306DB4E008
Malicious:	false
Preview:	.....$...,.....C.....p.....P.....,.....geips..... n.....lgoog.....R.....ozama.....onwod.....h...(.....g.bat... ....<...@.....uotpo.....X.....ennab.....nozam.....e..l....E.....-.....I...P.....,.....\|.....h...p...H...,.....\...X...T...P.....H .....@...<...8.....d...,...(...$.. .....,.....`...D.....|...x...t.....l...h...d...`.....X.....P...L...\...D. ..@...<...8...0...0..... .....`.....0.....h.....H...,.....x.....p...l...h...d...`...\...X...T...P...L...H...

C:\Users\user\AppData\Local\Google\Chrome\User Data\ce0c4376-afdc-4a6e-8309-8750a97ef5b6.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94772
Entropy (8bit):	3.749651061839044
Encrypted:	false
SSDEEP:	384:mb07Dh+g1KR9VKAHCNnrkvTZ30zRgH5QGoHryNXTxktNpsr2rmWC8O5HH/AON1PS:AeKl9Kd8lUeL7NdlnHOpKL53kV
MD5:	D2DB9AAC10198D30312FCEC0BF516DCF
SHA1:	49CB4115FAC8BAADDFB758E66C854B5B3045BC7B
SHA-256:	D5C0C93E9CB47A122416BA9AC352D0119A29972305CD0489F8623CA0396F8919
SHA-512:	7DD8F26799825CDF61CC7C812954A1A06B39A9D11BBC389E7F25AFF090AD4CE299F8112836CD861AB567308BF41BB5C2A5C8EC8CCCDC821E94108C27750E58 0
Malicious:	false
Preview:	0r.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....98.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\e99eab2a-d451-44bf-9c46-25844a558a2d.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	363510
Entropy (8bit):	6.027999735063634
Encrypted:	false
SSDEEP:	6144:9pubsIwHRYn8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBB:9AbOxzurRDn9nfNxF4ijZVtilBB
MD5:	1EAA2D372A6DA387C996928CF919E2D4
SHA1:	914D4FCE6ECBD2E09204F5629014CAF15F34A1D4
SHA-256:	6B105BFAB7B8C1E9837A8850590C44F50A3FDB338F8C186E5B171AE28CB8D60B
SHA-512:	F52568C150D35FE2A75587059865AD85B4AEDE5B4FEC5E960805B91B6D44803EC91A2058E7377F1531DB6F465CDA86C6CDC73F5587A8DD8694AAAD2A590694D
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620877810170619e+12,"network":1.62084541e+12,"ticks":116135456.0,"uncertainty":3250639.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075247322"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\eaf93029-4384-495d-b381-7187c73b4415.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	359931
Entropy (8bit):	6.015386152442761
Encrypted:	false
SSDEEP:	6144:mpubsIwHRYn8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBB:mAbOxzurRDn9nfNxF4ijZVtilBB

C:\Users\user\AppData\Local\Google\Chrome\User Data\eaf93029-4384-495d-b381-7187c73b4415.tmp	
MD5:	526B32F91D7C875AAF2EDDD06F358F00
SHA1:	6680134622D2F37BFE6FB9F8EF9A5B47519FC514
SHA-256:	562A8EDBD71EFAC1C56C504830CE6823A095E95905E4FBCFE331389F18114D69
SHA-512:	EB3369F5A1B242DB59FF31B8AD7ECAC301E9F45C7AFE3128D0852985B5ABABD5B4FA51F8AA4A259AF786DBE17536204D653BC7C3A8BFF8282B8ECCA0EEAB77F3
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620877810170619e+12,"network":1.62084541e+12,"ticks":116135456.0,"uncertainty":3250639.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"132653514054666

C:\Users\user\AppData\Local\Google\Chrome\User Data\fe679232-b176-4aa1-adff-aae6e75c7a2b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	359931
Entropy (8bit):	6.015385928114603
Encrypted:	false
SSDEEP:	6144:YpubsIwHRYn8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBB:YAbOxzurRDn9nfNxF4ijZVtilBB
MD5:	37B60688662B5A0D2F97F12056E631D5
SHA1:	59358EA1EADDD26E1E0CD710E501E3E869A926E3
SHA-256:	D4EE6633B265A5E1545BD6903A0605C930A6D65EDA4D6A158FBC9123CE2116A8
SHA-512:	02E5304157F9A67003943A2DF331F5D50852E1DE08D0E02A0F31C7B608819A80724D23D1C1D17B56120AB546E9FF387A3696F59322A78134F8FE4D5D3A30A722
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620877810170619e+12,"network":1.62084541e+12,"ticks":116135456.0,"uncertainty":3250639.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"132653514054666

C:\Users\user\AppData\Local\Temp\0943af95-bac0-4811-9f85-39bbbb00a164.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\1700_1014179753\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.89429824295036
Encrypted:	false
SSDEEP:	3:SRwGXyUtz24TSXhV6DDt5WBG9EBn:SGGXyA5kDoDt5WwaBn
MD5:	7FB6C0307DFC7235990A87216D6EFE79
SHA1:	9C86024DE6EE647227E73C5905468DB9C31D8447
SHA-256:	F01B98701AE70087F82AAC256AB3ECFB736F4865B7DF915051C7D5B1C51BA78E
SHA-512:	AC7106F2503DB666C4B3A382587C9DAE424CC5692D75E555D1F6BC0E4F4B3A360B82C1C356D06E4F607EA40206699191F5F206979E67B9614F1DE2073D5B0E40
Malicious:	false
Preview:	1.4dcc255c0d82123c9c4251bb453165672ea0458f0379f3a7a534dc2a666d7c6d

C:\Users\user\AppData\Local\Temp\1700_238488255\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.9669759926795995
Encrypted:	false
SSDEEP:	3:SfvHUTa8URTTH/BXDj6:SXD3TfB36
MD5:	E3EDA33A5C956F4FC9C5BBD91FF10252
SHA1:	182B989E299A3EC306622A9DD45C3B74A4DF6077
SHA-256:	6D7A462B703F1617286B65BFE0116F267328BEFC379812BCE774D8C640289647
SHA-512:	A49FF4979FEC3512C44899840CCF8D112806330C93812C515F09953B9B6DBA6B1DAB1828382D634235CF23E093C983AEFA860B7A75FDCB5F3F98DD928D4F47D
Malicious:	false
Preview:	1.d730fdd6875bfda19ae43c639e89fe6c24e48b53ec4f466b1d7de2001f97e03c

C:\Users\user\AppData\Local\Temp\1700_398063183\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.928261499316817
Encrypted:	false
SSDEEP:	3:STDLGswXEVBcVdBiTDt3zLsW:SPLGLErcVdBiDtf3
MD5:	C00BCE97F21B1AD61EB9B8CD001795EE
SHA1:	8E0392FF3DB267D847711C3F4E0D7468060E1535
SHA-256:	59F06F04230E32E8BC839F45B984D31D611930427B631C963D09E7064A602363
SHA-512:	9930E44A6ECC62505DBADCEED5E05645909FF09816FB12AAC0414E6D2830AC09758366C3B7D4EDD7839C87EB16DFA4C66D8981AE6237D408B37135C3506F4C2
Malicious:	false
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\user\AppData\Local\Temp\5fbd497d-ec92-40c3-bdb3-3692f707f885.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v....;.._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&..._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U .KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....I-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F ....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\68285ea9-b209-4598-81d9-61fbdaa927b6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false

C:\Users\user\AppData\Local\Temp\68285ea9-b209-4598-81d9-61fbdaa927b6.tmp	
Preview:	.

C:\Users\user\AppData\Local\Temp\79c209d2-8f54-4f9f-b818-cb5110b984aa.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\908ec0d7-8b6f-4061-a457-c031b12bb4dc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\cdd4e69e-6e17-4a5c-97ae-345b4f9ca12a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir1700_1680483029\908ec0d7-8b6f-4061-a457-c031b12bb4dc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false

C:\Users\user\AppData\Local\Temp\scoped_dir1700_1680483029\908ec0d7-8b6f-4061-a457-c031b12bb4dc.tmp	
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2…C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...I5....zJ.q.....L]....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir1700_1680483029\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
Malicious:	false
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1700_1680483029\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CEB4
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "Connecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1700_1680483029\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D84885B
Malicious:	false

C:\Users\user\AppData\Local\Temp\scoped_dir1700_1680483029\CRX_INSTALL_locales\cs\messages.json	
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed .".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1700_1680483029\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5 E0A
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_u navailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comp leted.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1700_1680483029\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB805 52
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_una vailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The trans action could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1700_1680483029\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B4
Malicious:	false
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavail able": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1700_1680483029\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593

C:\Users\user\AppData\Local\Temp\scoped_dir1700_1680483029\CRX_INSTALL_locales\en\messages.json	
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1700_1680483029\CRX_INSTALL_locales\en_GB\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

Static File Info

General

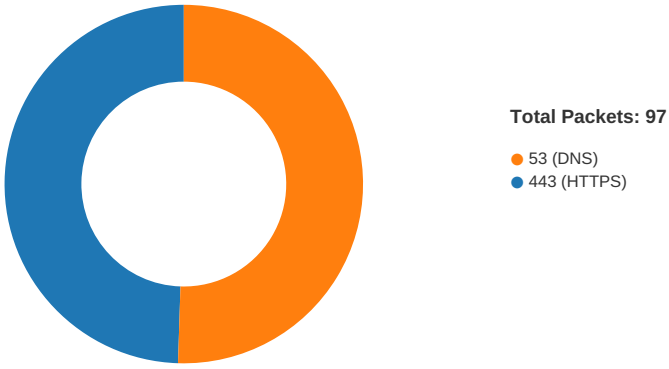
File type:	HTML document, ASCII text, with CRLF line terminators
Entropy (8bit):	4.960306832678102
TrID:	
File name:	#Ud83d#Udce0Lori's Fax VM-002.html
File size:	127
MD5:	dd018534b722864fa8404de333621478
SHA1:	e304a5ef3e4786cef59479da2ad59f69528763da
SHA256:	3c2937c71e855da9c18788eedf697d036b0ec62010f8b6ee2277696a8349d2ac
SHA512:	091ab44aafba6b79fd387a2127d6c163ff1a5beec8ab2a6073b6d89dfafd010f36a723bcc22555e5624b094c2dd6c98c2731c0a2122b5ca9df44b425fd13f0f8
SSDEEP:	3:gnkAqRAdrygovHcIIRVJbkADFoCDRTMS/GKtszKbdWpm3vIIb:7AqJH5IRjYmmMT/RaTIb
File Content Preview:	<script type="text/JavaScript">..setTimeout("location.href = 'https://doreenbrown.co.za/tele/cd?lori@cava.com';",0);..</script>

File Icon

Icon Hash:	e8d6a08c8882c461

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:50:10.363040924 CEST	49707	443	192.168.2.5	102.130.117.20
May 12, 2021 20:50:10.586344957 CEST	443	49707	102.130.117.20	192.168.2.5
May 12, 2021 20:50:10.586512089 CEST	49707	443	192.168.2.5	102.130.117.20
May 12, 2021 20:50:10.670161963 CEST	49707	443	192.168.2.5	102.130.117.20
May 12, 2021 20:50:10.893553972 CEST	443	49707	102.130.117.20	192.168.2.5
May 12, 2021 20:50:10.894314051 CEST	443	49707	102.130.117.20	192.168.2.5
May 12, 2021 20:50:10.894335032 CEST	443	49707	102.130.117.20	192.168.2.5
May 12, 2021 20:50:10.894351959 CEST	443	49707	102.130.117.20	192.168.2.5
May 12, 2021 20:50:10.894365072 CEST	443	49707	102.130.117.20	192.168.2.5
May 12, 2021 20:50:10.894433022 CEST	49707	443	192.168.2.5	102.130.117.20
May 12, 2021 20:50:10.897947073 CEST	443	49707	102.130.117.20	192.168.2.5
May 12, 2021 20:50:10.897967100 CEST	443	49707	102.130.117.20	192.168.2.5
May 12, 2021 20:50:10.898057938 CEST	49707	443	192.168.2.5	102.130.117.20
May 12, 2021 20:50:11.774502993 CEST	49707	443	192.168.2.5	102.130.117.20
May 12, 2021 20:50:11.774844885 CEST	49707	443	192.168.2.5	102.130.117.20
May 12, 2021 20:50:11.998774052 CEST	443	49707	102.130.117.20	192.168.2.5
May 12, 2021 20:50:11.998799086 CEST	443	49707	102.130.117.20	192.168.2.5
May 12, 2021 20:50:11.998868942 CEST	443	49707	102.130.117.20	192.168.2.5
May 12, 2021 20:50:11.998939991 CEST	49707	443	192.168.2.5	102.130.117.20
May 12, 2021 20:50:12.923667908 CEST	443	49707	102.130.117.20	192.168.2.5
May 12, 2021 20:50:12.932316065 CEST	49707	443	192.168.2.5	102.130.117.20
May 12, 2021 20:50:13.193567991 CEST	443	49707	102.130.117.20	192.168.2.5
May 12, 2021 20:50:13.287067890 CEST	443	49707	102.130.117.20	192.168.2.5
May 12, 2021 20:50:13.363845110 CEST	49707	443	192.168.2.5	102.130.117.20
May 12, 2021 20:50:13.559591055 CEST	49718	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:13.560254097 CEST	49719	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:13.611686945 CEST	49720	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:13.733620882 CEST	443	49719	199.79.62.225	192.168.2.5
May 12, 2021 20:50:13.733716011 CEST	49719	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:13.734030962 CEST	49719	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:13.734052896 CEST	443	49718	199.79.62.225	192.168.2.5
May 12, 2021 20:50:13.734158993 CEST	49718	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:13.734471083 CEST	49718	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:13.786206961 CEST	443	49720	199.79.62.225	192.168.2.5
May 12, 2021 20:50:13.786331892 CEST	49720	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:13.787336111 CEST	49720	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:13.907386065 CEST	443	49719	199.79.62.225	192.168.2.5
May 12, 2021 20:50:13.908883095 CEST	443	49718	199.79.62.225	192.168.2.5
May 12, 2021 20:50:13.910716057 CEST	443	49719	199.79.62.225	192.168.2.5
May 12, 2021 20:50:13.910762072 CEST	443	49719	199.79.62.225	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:50:13.910809040 CEST	443	49719	199.79.62.225	192.168.2.5
May 12, 2021 20:50:13.910902023 CEST	49719	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:13.911881924 CEST	443	49718	199.79.62.225	192.168.2.5
May 12, 2021 20:50:13.911928892 CEST	443	49718	199.79.62.225	192.168.2.5
May 12, 2021 20:50:13.911962986 CEST	443	49718	199.79.62.225	192.168.2.5
May 12, 2021 20:50:13.912009954 CEST	49718	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:13.957875013 CEST	49719	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:13.958620071 CEST	49718	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:13.962939978 CEST	443	49720	199.79.62.225	192.168.2.5
May 12, 2021 20:50:13.966073990 CEST	443	49720	199.79.62.225	192.168.2.5
May 12, 2021 20:50:13.966133118 CEST	443	49720	199.79.62.225	192.168.2.5
May 12, 2021 20:50:13.966173887 CEST	443	49720	199.79.62.225	192.168.2.5
May 12, 2021 20:50:13.966268063 CEST	49720	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.269639969 CEST	49719	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.270956039 CEST	49718	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.271981001 CEST	49720	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.272135973 CEST	49718	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.272214890 CEST	49720	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.272593975 CEST	49719	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.273049116 CEST	49719	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.443793058 CEST	443	49719	199.79.62.225	192.168.2.5
May 12, 2021 20:50:14.443831921 CEST	443	49719	199.79.62.225	192.168.2.5
May 12, 2021 20:50:14.443939924 CEST	49719	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.444036961 CEST	443	49719	199.79.62.225	192.168.2.5
May 12, 2021 20:50:14.444853067 CEST	49719	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.445843935 CEST	443	49718	199.79.62.225	192.168.2.5
May 12, 2021 20:50:14.445877075 CEST	443	49718	199.79.62.225	192.168.2.5
May 12, 2021 20:50:14.445979118 CEST	49718	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.446053028 CEST	49718	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.446073055 CEST	443	49718	199.79.62.225	192.168.2.5
May 12, 2021 20:50:14.446124077 CEST	49718	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.446319103 CEST	443	49719	199.79.62.225	192.168.2.5
May 12, 2021 20:50:14.446472883 CEST	443	49718	199.79.62.225	192.168.2.5
May 12, 2021 20:50:14.446523905 CEST	49718	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.446552038 CEST	443	49718	199.79.62.225	192.168.2.5
May 12, 2021 20:50:14.446573019 CEST	443	49719	199.79.62.225	192.168.2.5
May 12, 2021 20:50:14.446589947 CEST	443	49718	199.79.62.225	192.168.2.5
May 12, 2021 20:50:14.446599960 CEST	49718	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.446633101 CEST	49718	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.446712971 CEST	443	49720	199.79.62.225	192.168.2.5
May 12, 2021 20:50:14.446806908 CEST	49720	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.446916103 CEST	443	49720	199.79.62.225	192.168.2.5
May 12, 2021 20:50:14.446969986 CEST	49720	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.447192907 CEST	443	49720	199.79.62.225	192.168.2.5
May 12, 2021 20:50:14.447212934 CEST	443	49720	199.79.62.225	192.168.2.5
May 12, 2021 20:50:14.447231054 CEST	443	49720	199.79.62.225	192.168.2.5
May 12, 2021 20:50:14.447242975 CEST	49720	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.447263002 CEST	443	49720	199.79.62.225	192.168.2.5
May 12, 2021 20:50:14.447272062 CEST	49720	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.447278976 CEST	49720	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.447307110 CEST	49720	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.557884932 CEST	49719	443	192.168.2.5	199.79.62.225
May 12, 2021 20:50:14.653650999 CEST	443	49719	199.79.62.225	192.168.2.5
May 12, 2021 20:50:14.952588081 CEST	49707	443	192.168.2.5	102.130.117.20
May 12, 2021 20:50:15.163628101 CEST	443	49719	199.79.62.225	192.168.2.5
May 12, 2021 20:50:15.163650036 CEST	443	49719	199.79.62.225	192.168.2.5
May 12, 2021 20:50:15.163666964 CEST	443	49719	199.79.62.225	192.168.2.5
May 12, 2021 20:50:15.163681030 CEST	443	49719	199.79.62.225	192.168.2.5
May 12, 2021 20:50:15.163698912 CEST	443	49719	199.79.62.225	192.168.2.5
May 12, 2021 20:50:15.163713932 CEST	49719	443	192.168.2.5	199.79.62.225

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:49:56.242012024 CEST	54302	53	192.168.2.5	8.8.8.8
May 12, 2021 20:49:56.302180052 CEST	53	54302	8.8.8.8	192.168.2.5
May 12, 2021 20:49:56.366811991 CEST	53784	53	192.168.2.5	8.8.8.8
May 12, 2021 20:49:56.434855938 CEST	53	53784	8.8.8.8	192.168.2.5
May 12, 2021 20:49:56.442017078 CEST	65307	53	192.168.2.5	8.8.8.8
May 12, 2021 20:49:56.493268013 CEST	53	65307	8.8.8.8	192.168.2.5
May 12, 2021 20:49:56.531915903 CEST	64344	53	192.168.2.5	8.8.8.8
May 12, 2021 20:49:56.578533888 CEST	62060	53	192.168.2.5	8.8.8.8
May 12, 2021 20:49:56.593094110 CEST	53	64344	8.8.8.8	192.168.2.5
May 12, 2021 20:49:56.639823914 CEST	53	62060	8.8.8.8	192.168.2.5
May 12, 2021 20:49:57.352262020 CEST	61805	53	192.168.2.5	8.8.8.8
May 12, 2021 20:49:57.401148081 CEST	53	61805	8.8.8.8	192.168.2.5
May 12, 2021 20:49:58.134160995 CEST	54795	53	192.168.2.5	8.8.8.8
May 12, 2021 20:49:58.183134079 CEST	53	54795	8.8.8.8	192.168.2.5
May 12, 2021 20:49:59.285844088 CEST	49557	53	192.168.2.5	8.8.8.8
May 12, 2021 20:49:59.334693909 CEST	53	49557	8.8.8.8	192.168.2.5
May 12, 2021 20:50:01.703212023 CEST	61733	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:01.751802921 CEST	53	61733	8.8.8.8	192.168.2.5
May 12, 2021 20:50:02.567928076 CEST	65447	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:02.616869926 CEST	53	65447	8.8.8.8	192.168.2.5
May 12, 2021 20:50:03.758390903 CEST	52441	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:03.807318926 CEST	53	52441	8.8.8.8	192.168.2.5
May 12, 2021 20:50:09.884526968 CEST	65296	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:09.944533110 CEST	53	65296	8.8.8.8	192.168.2.5
May 12, 2021 20:50:10.059952974 CEST	63183	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:10.062525988 CEST	60151	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:10.069253922 CEST	56969	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:10.074429989 CEST	55161	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:10.126113892 CEST	53	55161	8.8.8.8	192.168.2.5
May 12, 2021 20:50:10.127391100 CEST	53	63183	8.8.8.8	192.168.2.5
May 12, 2021 20:50:10.127451897 CEST	53	60151	8.8.8.8	192.168.2.5
May 12, 2021 20:50:10.318463087 CEST	53	56969	8.8.8.8	192.168.2.5
May 12, 2021 20:50:10.795757055 CEST	54757	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:10.860955000 CEST	53	54757	8.8.8.8	192.168.2.5
May 12, 2021 20:50:10.912951946 CEST	49992	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:10.967874050 CEST	53	49992	8.8.8.8	192.168.2.5
May 12, 2021 20:50:11.006700039 CEST	60075	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:11.066509008 CEST	53	60075	8.8.8.8	192.168.2.5
May 12, 2021 20:50:11.068299055 CEST	55016	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:11.127801895 CEST	53	55016	8.8.8.8	192.168.2.5
May 12, 2021 20:50:12.198183060 CEST	64345	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:12.252090931 CEST	53	64345	8.8.8.8	192.168.2.5
May 12, 2021 20:50:13.362170935 CEST	50394	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:13.557322979 CEST	53	50394	8.8.8.8	192.168.2.5
May 12, 2021 20:50:13.699043036 CEST	58530	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:13.748002052 CEST	53	58530	8.8.8.8	192.168.2.5
May 12, 2021 20:50:15.476962090 CEST	53813	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:15.528465033 CEST	53	53813	8.8.8.8	192.168.2.5
May 12, 2021 20:50:15.854809046 CEST	63732	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:15.920483112 CEST	53	63732	8.8.8.8	192.168.2.5
May 12, 2021 20:50:17.147500038 CEST	57344	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:17.210560083 CEST	53	57344	8.8.8.8	192.168.2.5
May 12, 2021 20:50:22.828299999 CEST	57151	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:22.961535931 CEST	59413	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:23.016194105 CEST	53	57151	8.8.8.8	192.168.2.5
May 12, 2021 20:50:23.018591881 CEST	53	59413	8.8.8.8	192.168.2.5
May 12, 2021 20:50:23.181092978 CEST	60516	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:23.240854025 CEST	53	60516	8.8.8.8	192.168.2.5
May 12, 2021 20:50:24.577634096 CEST	51649	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:24.637734890 CEST	53	51649	8.8.8.8	192.168.2.5
May 12, 2021 20:50:25.450350046 CEST	65086	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:25.507559061 CEST	53	65086	8.8.8.8	192.168.2.5
May 12, 2021 20:50:40.325041056 CEST	56432	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:40.389839888 CEST	53	56432	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:50:50.846220016 CEST	52929	53	192.168.2.5	8.8.8.8
May 12, 2021 20:50:50.915376902 CEST	53	52929	8.8.8.8	192.168.2.5
May 12, 2021 20:51:06.762033939 CEST	64317	53	192.168.2.5	8.8.8.8
May 12, 2021 20:51:06.822146893 CEST	53	64317	8.8.8.8	192.168.2.5
May 12, 2021 20:51:07.481069088 CEST	56895	53	192.168.2.5	8.8.8.8
May 12, 2021 20:51:07.529911995 CEST	53	56895	8.8.8.8	192.168.2.5
May 12, 2021 20:51:07.670766115 CEST	62372	53	192.168.2.5	8.8.8.8
May 12, 2021 20:51:07.727909088 CEST	53	62372	8.8.8.8	192.168.2.5
May 12, 2021 20:51:08.714107037 CEST	61515	53	192.168.2.5	8.8.8.8
May 12, 2021 20:51:08.763088942 CEST	53	61515	8.8.8.8	192.168.2.5
May 12, 2021 20:51:10.205822945 CEST	56675	53	192.168.2.5	8.8.8.8
May 12, 2021 20:51:10.268018961 CEST	53	56675	8.8.8.8	192.168.2.5
May 12, 2021 20:51:17.756258965 CEST	57172	53	192.168.2.5	8.8.8.8
May 12, 2021 20:51:17.816445112 CEST	53	57172	8.8.8.8	192.168.2.5
May 12, 2021 20:51:23.795110941 CEST	55267	53	192.168.2.5	8.8.8.8
May 12, 2021 20:51:23.843967915 CEST	53	55267	8.8.8.8	192.168.2.5
May 12, 2021 20:51:23.973231077 CEST	50969	53	192.168.2.5	8.8.8.8
May 12, 2021 20:51:24.030441999 CEST	53	50969	8.8.8.8	192.168.2.5
May 12, 2021 20:51:24.176466942 CEST	64362	53	192.168.2.5	8.8.8.8
May 12, 2021 20:51:24.236793041 CEST	53	64362	8.8.8.8	192.168.2.5
May 12, 2021 20:51:41.492523909 CEST	54766	53	192.168.2.5	8.8.8.8
May 12, 2021 20:51:41.551130056 CEST	53	54766	8.8.8.8	192.168.2.5
May 12, 2021 20:51:48.553766012 CEST	61446	53	192.168.2.5	8.8.8.8
May 12, 2021 20:51:48.610667944 CEST	53	61446	8.8.8.8	192.168.2.5
May 12, 2021 20:52:01.166898966 CEST	57515	53	192.168.2.5	8.8.8.8
May 12, 2021 20:52:01.241837025 CEST	53	57515	8.8.8.8	192.168.2.5
May 12, 2021 20:52:21.476263046 CEST	58199	53	192.168.2.5	8.8.8.8
May 12, 2021 20:52:21.539684057 CEST	53	58199	8.8.8.8	192.168.2.5
May 12, 2021 20:52:30.756314993 CEST	65221	53	192.168.2.5	8.8.8.8
May 12, 2021 20:52:30.827950001 CEST	53	65221	8.8.8.8	192.168.2.5
May 12, 2021 20:52:50.027601957 CEST	61573	53	192.168.2.5	8.8.8.8
May 12, 2021 20:52:50.174959898 CEST	53	61573	8.8.8.8	192.168.2.5
May 12, 2021 20:52:52.032886028 CEST	56562	53	192.168.2.5	8.8.8.8
May 12, 2021 20:52:52.179039955 CEST	53	56562	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 20:50:10.069253922 CEST	192.168.2.5	8.8.8.8	0x8274	Standard query (0)	doreenbrown.co.za	A (IP address)	IN (0x0001)
May 12, 2021 20:50:13.362170935 CEST	192.168.2.5	8.8.8.8	0xc9eb	Standard query (0)	raghadstayl.com	A (IP address)	IN (0x0001)
May 12, 2021 20:50:15.854809046 CEST	192.168.2.5	8.8.8.8	0xeda9	Standard query (0)	logo.clearbit.com	A (IP address)	IN (0x0001)
May 12, 2021 20:50:22.828299999 CEST	192.168.2.5	8.8.8.8	0xc7a4	Standard query (0)	raghadstayl.com	A (IP address)	IN (0x0001)
May 12, 2021 20:50:22.961535931 CEST	192.168.2.5	8.8.8.8	0x4a6c	Standard query (0)	logo.clearbit.com	A (IP address)	IN (0x0001)
May 12, 2021 20:50:23.181092978 CEST	192.168.2.5	8.8.8.8	0x7037	Standard query (0)	clients2.google usercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 20:50:10.318463087 CEST	8.8.8.8	192.168.2.5	0x8274	No error (0)	doreenbrown.co.za		102.130.117.20	A (IP address)	IN (0x0001)
May 12, 2021 20:50:13.557322979 CEST	8.8.8.8	192.168.2.5	0xc9eb	No error (0)	raghadstayl.com		199.79.62.225	A (IP address)	IN (0x0001)
May 12, 2021 20:50:15.920483112 CEST	8.8.8.8	192.168.2.5	0xeda9	No error (0)	logo.clearbit.com	d26p066pn2w0s0.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:50:15.920483112 CEST	8.8.8.8	192.168.2.5	0xeda9	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.193.12	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 20:50:15.920483112 CEST	8.8.8.8	192.168.2.5	0xeda9	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.193.103	A (IP address)	IN (0x0001)
May 12, 2021 20:50:15.920483112 CEST	8.8.8.8	192.168.2.5	0xeda9	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.193.89	A (IP address)	IN (0x0001)
May 12, 2021 20:50:15.920483112 CEST	8.8.8.8	192.168.2.5	0xeda9	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.193.48	A (IP address)	IN (0x0001)
May 12, 2021 20:50:23.016194105 CEST	8.8.8.8	192.168.2.5	0xc7a4	No error (0)	raghadstayl.com		199.79.62.225	A (IP address)	IN (0x0001)
May 12, 2021 20:50:23.018591881 CEST	8.8.8.8	192.168.2.5	0x4a6c	No error (0)	logo.clearbit.com	d26p066pn2w0s0.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:50:23.018591881 CEST	8.8.8.8	192.168.2.5	0x4a6c	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.193.12	A (IP address)	IN (0x0001)
May 12, 2021 20:50:23.018591881 CEST	8.8.8.8	192.168.2.5	0x4a6c	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.193.103	A (IP address)	IN (0x0001)
May 12, 2021 20:50:23.018591881 CEST	8.8.8.8	192.168.2.5	0x4a6c	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.193.89	A (IP address)	IN (0x0001)
May 12, 2021 20:50:23.018591881 CEST	8.8.8.8	192.168.2.5	0x4a6c	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.193.48	A (IP address)	IN (0x0001)
May 12, 2021 20:50:23.240854025 CEST	8.8.8.8	192.168.2.5	0x7037	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:50:23.240854025 CEST	8.8.8.8	192.168.2.5	0x7037	No error (0)	googlehosted.l.googleusercontent.com		216.58.212.129	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 20:50:23.121891022 CEST	13.224.193.12	443	192.168.2.5	49742	CN=clearbit.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Apr 22 02:00:00 CEST 2021	Sun May 22 01:59:59 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 20:50:23.367300034 CEST	199.79.62.225	443	192.168.2.5	49741	CN=webmail.raghadstayl.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Mar 23 12:08:39 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Jun 21 13:08:39 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 12, 2021 20:50:23.368551970 CEST	199.79.62.225	443	192.168.2.5	49740	CN=webmail.raghadstayl.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Mar 23 12:08:39 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Jun 21 13:08:39 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior

chrome.exe
chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 1700 Parent PID: 3900

General

Start time:	20:50:04
Start date:	12/05/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\#Ud83d#Udce0Lori's Fax VM-002.html'
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: 6332 Parent PID: 1700

General

Start time:	20:50:07
Start date:	12/05/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1508,17710434684604522590,2061890025822799301,31072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1940 /prefetch:8
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly